Copyright and Trademark Information

Fujitsu Computer Systems Corporation has made every effort to ensure the accuracy and completeness of this document. Because ongoing development efforts are made to continually improve the capabilities of our products, however, the data contained herein represents Fujitsu design objectives and is provided for comparative purposes; actual results may vary based on a variety of factors. This product data does not constitute a warranty. Specifications are subject to change without knowledge.

Fujitsu and the Fujitsu logo are registered trademarks of Fujitsu Limited; Stylistic is a registered trademark of Fujitsu Computer Systems Corporation.

Microsoft and Windows are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

PCMCIA and CardBus are registered trademarks of the Personal Computer Memory Card International Association.

Intel, Pentium, and SpeedStep are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Atheros is a registered trademark of Atheros Communications, Inc.

Bluetooth and the Bluetooth logo are registered trademarks of Bluetooth SIG, Inc.

Memory Stick is a registered trademark of Sony Corporation and/or its affiliates

Wi-Fi is a trademark of the Wireless Ethernet Compatibility Alliance (WECA).

All other products are trademarks or registered trademarks of their respective companies.

Warning

Handling the cord on this product will expose you to lead, a chemical known to the State of California to cause birth defects or other reproductive harm.

Wash hands after handling.

B6FH-6891-01EN-00

DECLARATION OF CONFORMITY according to FCC Part 15

Responsible Party Name:	**Fujitsu Computer Systems Corporation**
Address:	**1250 E. Arques Avenue, MS 122** **Sunnyvale, CA 94085**
Telephone:	**408-746-6000**
Declares that product:	**Model Series: Stylistic® ST5000 Tablet PC** **Complies with Part 15 of the FCC Rules**

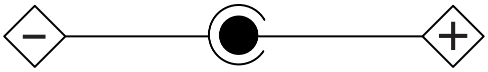
This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and, (2) This device must accept any interference received, including interference that may cause undesired operation.

Note: *For more detailed information about the FCC rules and their applicability to the Stylistic ST5000 Series Tablet PC, refer to Chapter 5 of this document.*

IMPORTANT SAFETY INSTRUCTIONS

- This unit requires an AC adapter to operate. Use only UL Listed Class 2 Adapters with an output rating of 16 VDC, with a current of 3.75A minimum.

AC Adapter output polarity:



- When using your notebook equipment, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:
  - Do not use this product near water for example, near a bathtub, washbowl, kitchen sink or laundry tub, in a wet basement or near a swimming pool.
  - Avoid using the modem during an electrical storm. There may be a remote risk of electric shock from lightning.
  - Do not use the modem to report a gas leak in the vicinity of the leak.
  - Use only the power cord and batteries indicated in this manual. Do not dispose of batteries in a fire. They may explode. Check with local codes for possible special disposal instructions.
- To reduce the risk of fire, use only No. 26 AWG or larger UL Listed or CSA Certified Telecommunication Line Cord

SAVE THESE INSTRUCTIONS

For Authorized Repair Technicians Only

⚠ Danger of explosion if Lithium (clock) battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instruction.

⚠ For continued protection against risk of fire, replace only with the same type and rating fuse.

System Disposal

Hg LAMP(S) INSIDE THIS PRODUCT CONTAIN MERCURY AND MUST BE RECYCLED OR DISPOSED OF ACCORDING TO LOCAL, STATE, OR FEDERAL LAWS.

Table of Contents

PREFACE

1

GETTING STARTED

Getting Started with Your Tablet PC

2

USING YOUR TABLET PC

Using the ST5000 Series Tablet PC

3

CARING FOR YOUR TABLET PC

Care and Maintenance

4

SYSTEM SPECIFICATIONS

ST5000 Series Hardware Specifications

Regulatory Information

APPENDIX A: WIRELESS LAN/ BLUETOOTH USER'S GUIDE

Before Using the Wireless LAN

Connecting the WLAN

Other settings

WLAN Troubleshooting

Wireless LAN Glossary

IP address information

Specifications

Using the Bluetooth Device

APPENDIX B: SECURITY DEVICE USER'S GUIDE

Fingerprint Sensor Device

Trusted Platform Module Installation

Index

Preface

Preface

ABOUT THIS GUIDE

The Stylistic® ST5000 Series Tablet PC is a high-performance, pen-based computer that has been designed to support Microsoft®Windows® XP Tablet PC Edition.

This manual explains how to operate your Fujitsu Stylistic ST5000 Series Tablet PC hardware and built-in system software.

The Stylistic ST5000 Series Tablet PC is a completely self-contained unit with an active-matrix (TFT) color LCD display and an active digitizer. It has a powerful interface that enables it to support a variety of optional features.

Conventions Used in the Guide

Keyboard keys appear in brackets.
Example: [Fn], [F1], [ESC], [ENTER] and [CTRL].

Pages with additional information about a specific topic are cross-referenced within the text.
Example: (See page xx.)

On screen buttons or menu items appear in bold
Example: Click **OK** to restart your Tablet PC.

DOS commands you enter appear in Courier type.
Example: `Shut down the computer?`

The information icon highlights information that will enhance your understanding of the subject material.

The caution icon highlights information that is important to the safe operation of your computer, or to the integrity of your files. Please read all caution information carefully.

The warning icon highlights information that can be hazardous to either you, your computer, or your files. Please read all warning information carefully.

FUJITSU CONTACT INFORMATION

Service and Support

You can contact Fujitsu Service and Support in the following ways:

- Toll free: 1-800-8Fujitsu (1-800-838-5487)
- E-mail: 8fujitsu@us.fujitsu.com
- Web site:
  http://www.computers.us.fujitsu.com/support

Before you place the call, you should have the following information ready so the customer support representative can provide you with the fastest possible solution:

- Product name
- Product configuration number
- Product serial number
- Purchase date
- Conditions under which the problem occurred
- Any error messages that have occurred
- Type of device connected, if any

Fujitsu Online

You can go directly to the online Fujitsu product catalog for your Stylistic Tablet PC by clicking on the Fujitsu Weblinks -> LifeBook Accessories web site link, located in the Windows Start -> All Programs menu.

You can also reach Fujitsu Service and Support on-line by clicking on the Fujitsu Weblinks -> Fujitsu Service and Support Web site link, located in the Service and Support Software folder of the Windows Start -> All Programs menu..

You must have an active internet connection to use the online URL links.

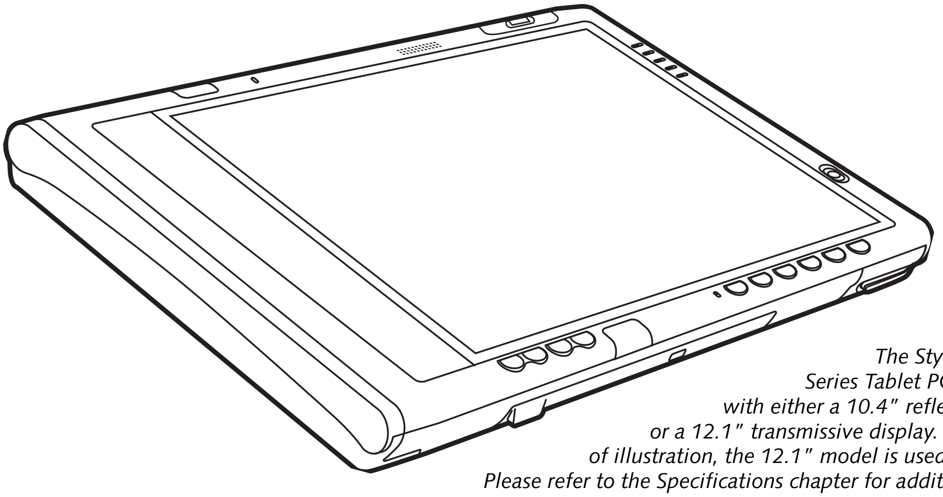
LIMITED WARRANTY INFORMATION

Your Stylistic ST5000 Series Tablet PC is backed by an International Limited Warranty. Check the service kit that came with your system for warranty terms and conditions.

1

Getting Started with Your Tablet PC

Getting Started with Your Stylistic Tablet PC



The Stylistic ST5000 Series Tablet PC is available with either a 10.4" reflective display or a 12.1" transmissive display. For purposes of illustration, the 12.1" model is used throughout. Please refer to the Specifications chapter for additional details.

Figure 1-1. Stylistic ST5000 Series Tablet PC

The Stylistic® ST5000 Series Tablet PC is a high-performance, pen-based computer that has been designed to support Microsoft® Windows® XP Tablet PC Edition 2005. This chapter provides an overview of the Stylistic ST5000 Series Tablet PC and its features.

IN-BOX ITEMS FOR THE STYLISTIC ST5000 SERIES TABLET PC

Verify that the following items are included in the box with your Tablet PC:

- Stylistic ST5000 Series active pen
- Pen tips (quantity: 5)
- Pen tip removal tool
- Pen tether
- Main battery
- Power cord
- AC adapter
- Screen protectors (quantity: 2)
- Getting Started Guide
- Quick Tips Guide
- Drivers and Application Restore (DAR) DVD
- System Restore DVD

OPTIONAL ACCESSORIES

The following optional accessories can be used with the Stylistic ST5000 Series Tablet PC. Refer to the instructions provided with these accessories for details on their use.

For the latest list of accessories available for your Tablet PC, be sure to frequently check the Fujitsu Web site at: www.shopfujitsu.com.

Peripheral/Accessory	
Docking Options	
Tablet PC Tablet Dock, with CD-ROM drive	Universal Dock Mount
Tablet PC Tablet Dock, with Combo DVD/CD-RW drive	Folding Desk Stand
Charge-Only Cradle	
Carrying Cases	
Tablet PC Executive Leather Portfolio Case	Bump Case
Tablet PC Nylon Attaché Case	Easel Case
Harsh Environment Case (HEC)	Hand Strap
Media Options	
External USB Floppy Disk Drive	USB CD-ROM Drive
External DVD/CD-ROM Combo Drive	
Memory	
256 MB SO DIMM, DDR2 400 MHz	128 MB Compact Flash Card
512 MB SO DIMM, DDR2 400 MHz	256 MB Compact Flash Card
1 GB SO DIMM, DDR2 400 MHz	128 MB Secure Digital Memory Card
Power Options	
AC Adapter with US Cord	Auto/Airline Adapter
Main Battery	Battery Charger
High-Capacity Battery	
Input Devices	
Wireless Keyboard	USB Optical Mouse
Wireless Keyboard with Touchpad	Stylistic ST5000 Tablet PC Pen (2-pack)
Logitech Wireless Keyboard and Mouse	Wireless Mouse with Scroll Function
Additional Accessories	
Screen Protectors (6-pack)	Compact Flash Card Adapter
HEC Screen Protectors (2-pack)	Notebook Guardian Lock
4 in 1 PC Card Adapter (SD/MMC/ Memory Stick/SmartMedia)	Deluxe Pen Tether
	Charge-Only Cradle DC Adapters

Table 1-1. Stylistic ST5000 Series Optional Accessories

STYLISTIC TABLET PC FEATURES

Features and controls that you use to operate the Stylistic ST5000 Series Tablet PC are outlined below and illustrated in Figures 1-1 through 1-6. Details on using these features and controls are provided later in this manual.

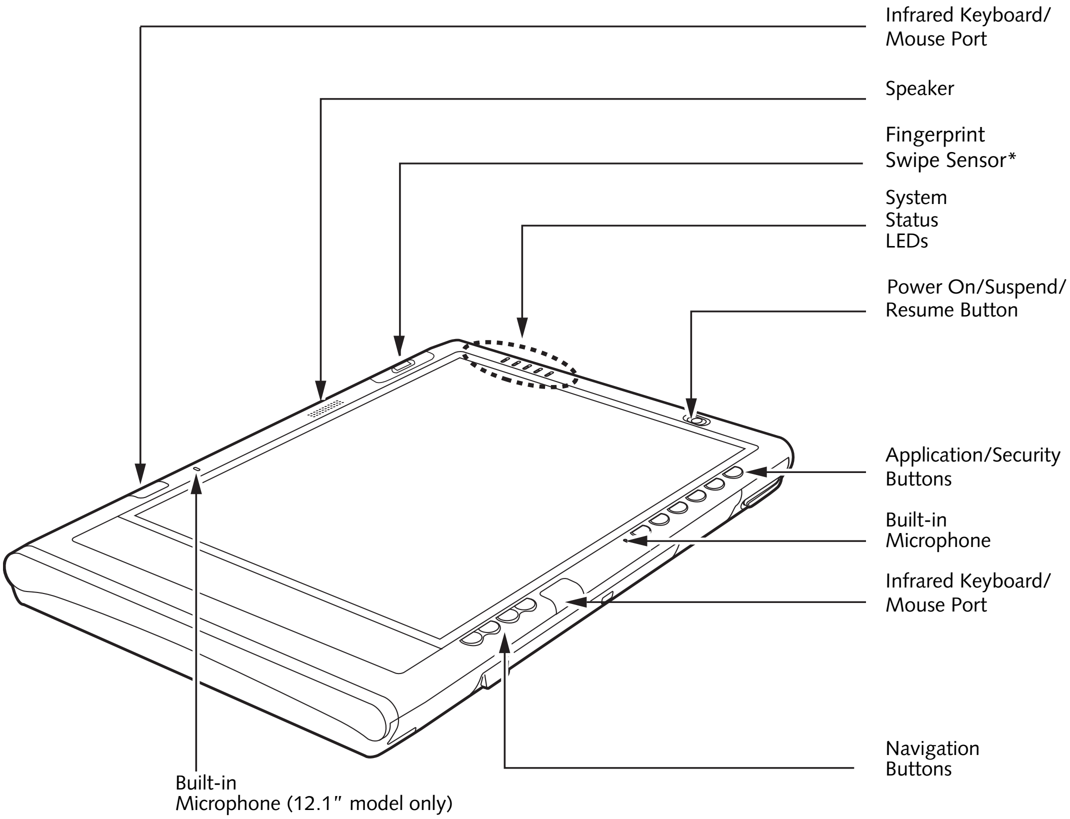

Infrared Keyboard/ Mouse Port
Speaker
Fingerprint Swipe Sensor*
System Status LEDs
Power On/Suspend/ Resume Button
Application/Security Buttons
Built-in Microphone
Infrared Keyboard/ Mouse Port
Navigation Buttons
Built-in Microphone (12.1" model only)

Figure 1-2. Stylistic ST5000 Series Tablet PC Features (Front View)

Front Features:

- **Infrared keyboard/mouse ports**: The infrared ports are used for communicating with a proprietary infrared keyboard or mouse.†
- **Speaker:** Allows you to listen to mono audio files.
- **Fingerprint Swipe Sensor*:** The optional fingerprint swipe sensor allows you to start your system by swiping your finger over the sensor.
- **System status LEDs:** Indicate the operational status of the Tablet PC and hard disk drive, the charge level of the battery, and the security panel.
- **Power On/Suspend/Resume button:** Allows you to turn on, off, suspend, resume, hibernate or wake the Tablet PC in order to optimize battery life.
- **Application buttons:** Allow you to quickly launch pre-defined applications, utilities, and security features by pressing a button.
- **Navigation buttons:** The navigation buttons allow you to move: Page Up/Page Down, Tab Right/Tab Left, Cursor Up/Cursor Down, and Cursor Right/ Cursor Left.
- **Built-in Microphones:** The built-in microphone(s) allow you to input mono audio. Note that the 10.4” model has only one microphone.

† These peripherals and accessories are sold separately.

* The fingerprint swipe sensor is available only on the 12.1” model.

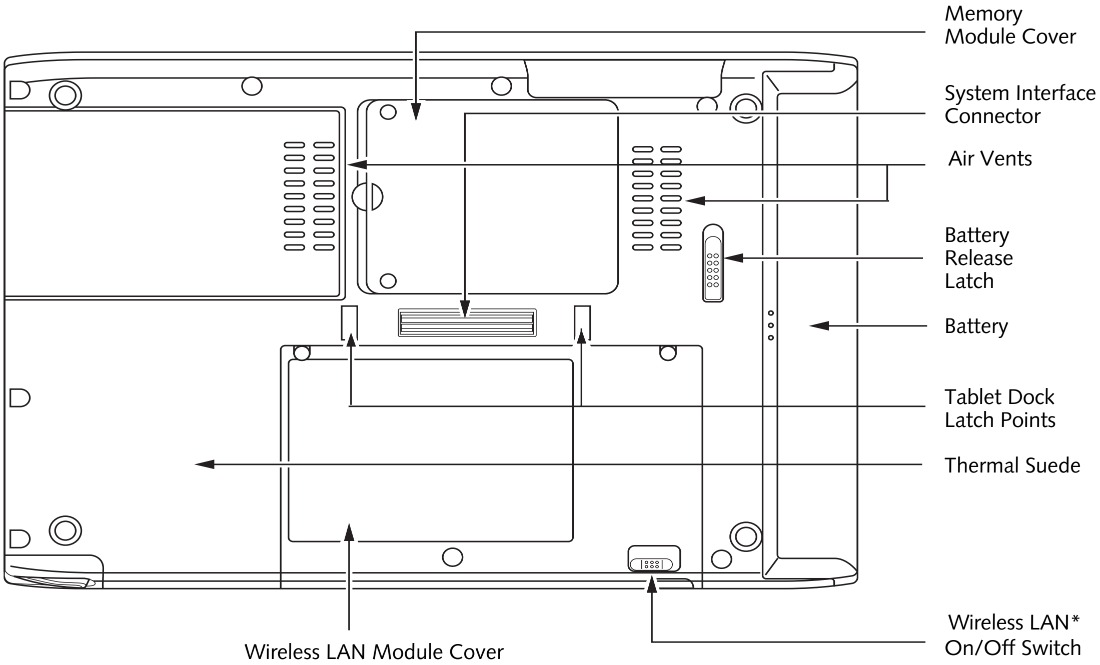


Figure 1-3. Stylistic ST5000 Series Tablet PC Features (Back View)

Back Features:

- **System interface connector:** Allows you to connect the optional Stylistic Tablet Dock.†
- **Removable battery:** Can be removed and replaced with a charged battery.†
- **Battery release latch:** Used to release the removable battery.
- **Tablet Dock latch point:** Allows you to attach the system to an optional Tablet Dock.†
- **Memory module cover:** Removable cover over the memory modules.
- **Thermal Suede:** Several areas of the system back are covered with "thermal suede". This material should **not** be removed. It is designed to minimize the heat that the user feels when the system has been operating for an extended period of time.

Air Vents: The air vents assist in proper cooling of the syatem.

⚠ To protect your notebook from damage and to optimize system performance, be sure to **keep all air all vents unobstructed, clean, and clear of debris**. This may require periodic cleaning, depending upon the environment in which the system is used.

Do not operate the notebook in areas where the air vents can be obstructed, such as in tight enclosures or on soft surfaces like a bed or cushion.

- **Wireless LAN module cover:** Provides protection for the optional wireless LAN radio.
- **Wireless LAN/Bluetooth On/Off switch:** For systems with the optional wireless LAN radio or Bluetooth device, this switch toggles the radio on or off.

† These peripherals and accessories are sold separately.

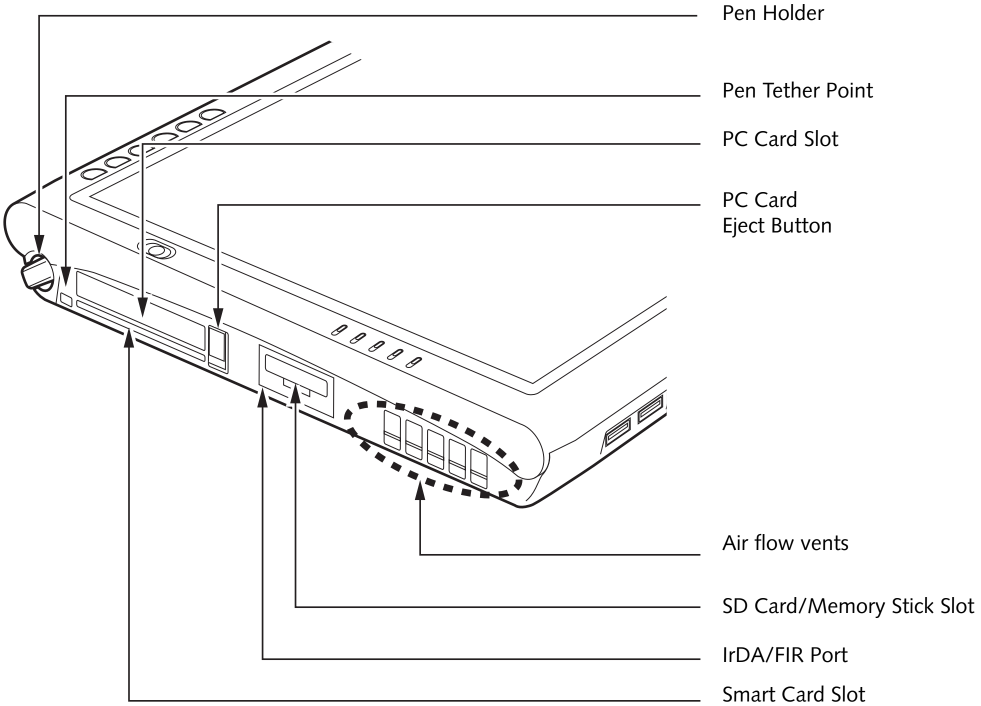


Figure 1-4. Stylistic ST5000 Series Tablet PC Features (Top View)

Top Features:

- **Pen:** The main input device that you use to execute programs and enter data. A pen holder is built into the Tablet PC to store the pen when not in use.
- **Pen Tether Point:** The pen tether point is used to attach a pen tether to help prevent loss of the pen.
- **PC Card slot:** Allows you to insert a Type I or Type II PCMCIA Card† in the system.
- **PC Card Eject Button:** The PC Card eject button is used to remove a PC Card from the PC Card slot.
- **Air flow vents:** Provides secondary cooling for processor.

To protect your notebook from damage and to optimize system performance, be sure to **keep all air all vents unobstructed, clean, and clear of debris**. This may require periodic cleaning, depending upon the environment in which the system is used.

Do not operate the notebook in areas where the air vents can be obstructed, such as in tight enclosures or on soft surfaces like a bed or cushion.

- **SD Card/Memory Stick Slot:** The Secure Digital (SD) card/Memory Stick slot allows you to insert a flash memory card† for data storage. Flash memory cards allow you to transfer data to and from a variety of different digital devices.
- **IrDA/FIR port:** Provides an infrared interface for communication with devices compliant with IrDA Standard Revision 1.1.
- **Smart Card Slot:** The dedicated Smart Card slot allows you to insert a Smart Card† on which you can store such data as medical information or electronic “cash”.

† These peripherals and accessories are sold separately.

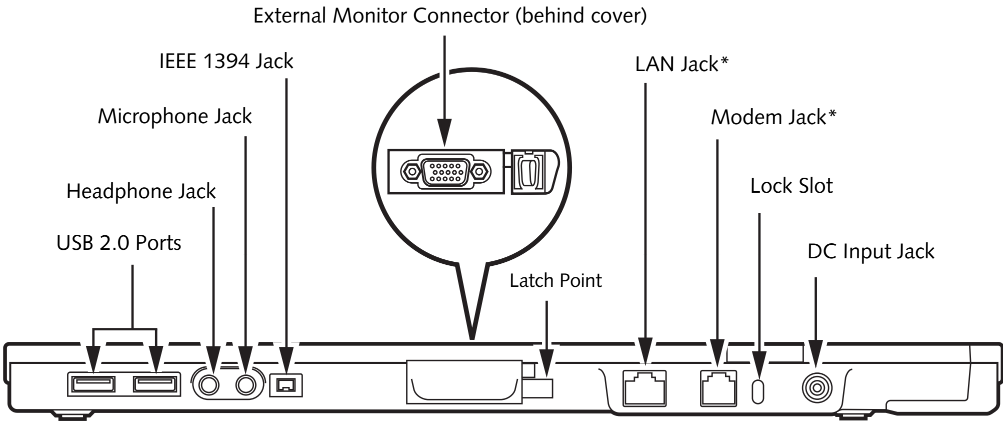


Figure 1-5. Stylistic ST5000 Series Tablet PC Features (Left Side View)

Left-Side Features:

- **USB 2.0 ports:** Allow you to connect Universal Serial Bus-compliant devices (compliant with USB Standard Revision 2.0) to the Tablet PC. Additional USB ports are located on the optional Tablet Dock†.
- **Headphone Jack:** Allows you to connect a set of stereo headphones†.
- **Microphone Jack:** Allows you to connect an external microphone†.
- **IEEE 1394 Jack:** Allows you to connect IEEE 1394 (Firewire) peripherals such as digital video cameras† or external hard drives† to your Tablet PC.
- **External Monitor Connector:** The External Monitor connector allows you to connect an external VGA, XGA, or SVGA CRT monitor.
- **Modem jack:** Allows you to connect a standard RJ-11 connector to the Tablet PC's internal 56 Kbps modem. Note that the internal 56 Kbps modem module installed in the Stylistic ST5000 Series Tablet PC has actual maximum transfer rates of 53 Kbps (receive), 33.6 Kbps (send), and 14.4 Kbps (fax). Download rates are limited to 53 Kbps in the United States due to FCC restrictions.
- **LAN jack:** Allows you to connect a standard RJ-45 connector to the Tablet PC's internal local area network (LAN).
- **Lock slot**: Allows you to attach a compatible security cable.†
- **DC input connector:** Allows you to connect the AC adapter or auto adapter.†

† These peripherals and accessories are sold separately.

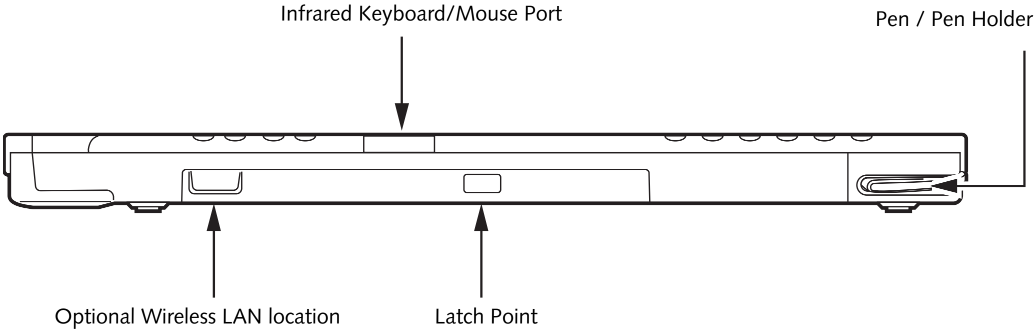


Figure 1-6. Stylistic ST5000 Series Tablet PC Features (Right Side View)

Right-Side Features:

- **Pen:** The main pointing device that you use to execute programs and enter data. A pen holder is built into the Tablet PC to store the pen when not in use.
- **Infrared keyboard/mouse port**: The infrared port wraps around the front and bottom of the display, and is used for communicating with an optional proprietary infrared keyboard or mouse†.
- **Wireless LAN location:** The optional wireless LAN device is located inside of the system housing.

† These peripherals and accessories are sold separately.

STATUS DISPLAY

Icons appear under each of the system status LEDs in the status display indicating the status of system functions such as system power and battery charge level. The location of icons in the Status display is shown in Figure 1-7.

Table 1-2. explains how the LEDs associated with the individual icons are displayed, and describes what the variations of that display indicate. (If an icon is not displayed, it indicates that the related system function is off or inactive.

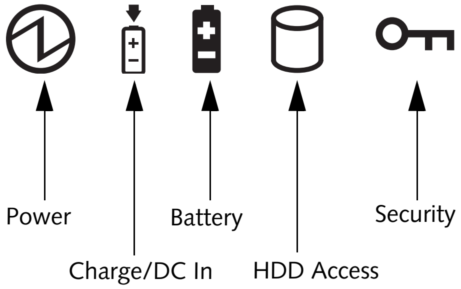


Figure 1-7. Status Display Icons

In the following table, a "blinking" LED flashes at the rate of once per second; an LED that is "blinking, slow" flashes at the rate of one second on, five seconds off.

Icon	Mode/State	LED State	Remarks
Power	• On State • Idle Mode	Green, continuous	The system is powered on and ready for use.
	• Suspend-to-RAM	Green, blinking	The system has suspended and saved active settings to RAM.
	• Off State • Hibernate (Save-to-Disk)	Off	The system has suspended and saved settings and data to the hard disk drive.
Charge/DC In	• On State • Idle Mode • Suspend-to-RAM • Hibernate (Save-to-Disk) • Off State	Amber	AC adapter and battery are available and system is charging.
		Green	• AC adapter and battery are available and system is not charging (battery fully charged). • AC adapter is available but battery is not present.
		Amber, blinking	AC adapter and battery are available and waiting to charge (battery is out of thermal range).
		Off	AC adapter is not available.

In the following table, a “blinking” LED flashes at the rate of once per second; an LED that is “blinking, slow” flashes at the rate of one second on, five seconds off.

Icon	Mode/State	LED State	Remarks
Battery 🔋	• On State • Idle Mode	Green, continuous	Battery charge is between 50%-100%
		Amber, continuous	Battery charge is between 13%-49%
		Red, continuous	Battery charge is between 0%-12%
		Red, blinking	There is a battery error.
	• Suspend-to-RAM, without AC adapter • Suspend-to-RAM with AC adapter	Green, blinking slow	Battery charge is between 50%-100%.
		Amber, blinking slow	Battery charge is between 13%-49%.
		Red, blinking slow	Battery charge is between 0%-12%.
	• Hibernate (Save-to-Disk), with AC adapter • Off State	Off	Battery is not installed, or system is off or in Hibernate mode.
	• Hibernate (Save-to-Disk), without AC adapter		If battery is inserted during power off, LED blinks amber for 4 seconds to detect battery. Battery status is displayed for 5 seconds after that.
HDD Access ⛁	• On State (or flashing) • Idle Mode	Green	Displayed when hard disk drive is accessed.
	• Suspend-to-RAM • Hibernate (Save-to-Disk) • Off State	Off	Hard disk drive is not being accessed.
Security 🔑	• On State	Green, continuous (until password is entered)	The Security Indicator lights (if a password was set) when the system resumes from Off or Standby modes. You must enter the password that was set in the Security Panel before your system will resume operation. *(See Security Functions of Application Buttons on page 14 for more information.)*

Table 1-2. System Status Indicators

APPLICATION BUTTONS

The six application buttons are located on the upper right-hand side of a vertically-oriented system. *(See figure 1-2 on page 3 for location)*. Five of the buttons have secondary functions. The secondary functions are activated by pressing the Function (Fn) button while pressing the application button.

The buttons also have separate tertiary functions that can be used while the system is booting up. For more information about the tertiary functions, refer to Table 1-5 on page 13.

Ctl-Alt-Del is the only application button that can be used while the system is logging on or when the system is locked (i.e., when you have the Logon or Computer Locked window showing on your desktop).

Button Icon and Name (Primary)	Tablet Icon (Fn + Button) (Secondary)	Description
Alt **Ctl-Alt-Del Button**	🔑 **Security Button**	Pressing the **Ctl-Alt-Del** button for approximately one second allows you to log on after boot or after resuming from power management. **Security Button:** All five buttons are used when implementing security functions. Four of the buttons are used to enter the password, and the fifth is used as an Enter button. See "Security Functions of Application Buttons" on page 14.
✉ **EMail Button**	🪐 **Internet Button**	When you press the **EMail** button, you automatically launch Microsoft Outlook Express, where you can read, create, and send emails. When you press the **Fn + EMail** buttons at the same time, you automatically launch the Web browser. The default page to which you go is the Fujitsu home page. If you would like to change your home page, go to the Control Panel-> Internet Options. Select the General tab and enter the starting address you would like to use.
⧉ **Orientation Button**	▢ **Display Mode Button**	When you press the **Orientation** button, the system screen orientation changes from portrait (vertical) to landscape (horizontal) or from landscape to portrait. When you would like to use the Tablet PC as an eBook, for example, you would use the portrait orientation, when accessing spreadsheets, you would more typically use a landscape orientation. When you press the **Fn + Orientation** buttons at the same time*, the display output will switch between internal, external, and simultaneous display.
ESC **Escape Button**	A **Application A Button**	The **Escape** application button acts the same way as an Escape key on a keyboard. When you press the **Fn + Esc** buttons at the same time*, they act to invoke a pre-determined application or generate a combination keystroke, as assigned in the Tablet Button Settings utility. (You can change the settings in **Control Panel -> Tablet Button Settings**). By default, pressing the **Fn + Esc** combination acts the same as if you had pressed **Ctl + Esc** on a keyboard: the Start menu is launched.

Button Icon and Name (Primary)	Tablet Icon (Fn + Button) (Secondary)	Description
ENT Enter Button	B Application B Button	The **Enter** application button acts the same way as an Enter key on a keyboard. Pressing the **Fn + Ent** buttons at the same time*, acts to invoke a pre-determined application or keystroke combination, as assigned in the Tablet Button Settings utility. (You can change the settings in **Control Panel** -> **Tablet Button Settings**). By default, pressing the **Fn + Ent** combination acts the same as if you had pressed **Alt** on a keyboard: it selects a main menu in the typical Windows application.
Fn Function Button	Fujitsu Menu Utility	The **Function** button works in conjunction with the other application buttons to provide additional functionality for the buttons. Refer to specific details above.* Pressing the **Fn** button twice in succession (within the "sticky" time*), causes the Fujitsu menu to appear on your screen, allowing you to modify certain system settings.

Table 1-3. Application Buttons - Primary and Secondary Functions

* The **Fn** button has a handy "sticky" feature that allows you to press two buttons in immediate succession, rather than at exactly the same time. After pressing the **Fn** button, you have a short time (2 to 3 seconds) to press the second button.

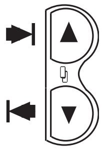
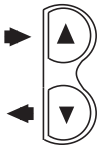
NAVIGATION BUTTONS

The two navigation buttons are located on the lower right-hand side of a vertically-oriented system. *(See figure 1-2 on page 3 for location)*. Each of the buttons can be toggled by pressing either end of the button.

The buttons have dual functions. The secondary functions are activated by pressing the Function (Fn) button while pressing the application button*.

The buttons also have separate tertiary functions that can be used while the system is booting up. For more information about the tertiary functions, refer to Table 1-5 on page 13.

Ctl-Alt-Del is the only Application button that can be used while the system is logging on or when the system is locked (i.e., when you have the Logon or Computer Locked window showing on your desktop).

Buttons/icons	Purpose (when pressed alone) ("Primary" function)	Purpose (when pressed with Fn button) ("Secondary" function)
	This button consists of Page Up and Page Down segments. When the Page Up portion is pressed, you will scroll up one page. When the Page Down portion is pressed, you will scroll down one page.	When pressed with the Function (Fn) button*, the Up portion of this button allows you to tab right. When pressed with the Function (Fn) button*, the Down portion of this button allows you to tab left.
	This button consists of Up and Down segments. When the Up portion is pressed, the cursor will move up. When the Down portion is pressed, the cursor will move down.	When pressed with the Function (Fn) button*, the Up portion of this button will move the cursor to the right. When pressed with the Function (Fn) button*, the Down portion of this button will move the cursor to the left.

* The **Fn** button has a handy "sticky" feature that allows you to press two buttons in immediate succession, rather than at exactly the same time. After pressing the **Fn** button, you have a short time (2 to 3 seconds) to press the second button.

Table 1-4. Navigation Buttons

TERTIARY FUNCTIONS OF APPLICATION AND NAVIGATION BUTTONS

While you are booting up your system, the Application Buttons and Navigation buttons can be used for entering and navigating through the Basic Input-Output System (BIOS), and for invoking the Advanced Options Menu, where you can enter different modes (such as Safe Mode).

The BIOS is a program and a set of parameters that are stored in ROM, which tests and operates your Tablet PC from when you turn it on until it loads your installed operating system from disk. Information from the BIOS is transferred to the operating system to provide it with information on the configuration and status of the hardware.

The system is booting up while the Fujitsu logo is displayed immediately after turning on the system. The table below indicates how the buttons act while the system is booting up and while you are in the BIOS.

Buttons/icons	Purpose (when pressed while the system is booting up)
Alt **Ctl-Alt-Del Button**	Pressing the **Ctl-Alt-Del** button while the system is booting up takes you into BIOS setup. This is the same as if you had tapped [**F2**] on a keyboard.
✉ **EMail Button**	Pressing the **EMail** button while the system is booting up opens the Boot Options menu. This is the same as if you had tapped [**F12**] on a keyboard.
⧉ **Orientation Button**	Pressing the **Orientation** button while the BIOS setup screen is open causes the selected item (if applicable) to change to the next item. Pressing this is the same as tapping the spacebar on a keyboard.
ESC **Escape Button**	Pressing the **Esc** button while the BIOS is open acts to escape from the BIOS. This is the same as if you had tapped [**Esc**] on a keyboard.
ENT **Enter Button**	Pressing the **Ent** button while the BIOS is open acts the same as the [**Ent**] button on a keyboard.
Fn **Function Button**	Pressing the **Fn** button while the system is displaying the operating system boot menu, opens the Advanced Operating System Options menu. This menu allows you to enter different operating system modes (such as Safe Mode). Pressing this button is the same as if you had tapped [**F8**] on a keyboard.
⇥ ▲ ⇤ ▼	Pressing the top half of the upper navigation button while the BIOS setup screen is open causes the cursor in the BIOS setup screen to move up. This is the same as if you had tapped Arrow Up on a keyboard. This feature is also functional in the operating system boot menu.
	Pressing the bottom half of the upper navigation button while the BIOS setup screen is open causes the cursor in the BIOS setup screen to move down. This is the same as if you had tapped Arrow Down on a keyboard. This feature is also functional in the operating system boot menu.
▶ ▲ ◀ ▼	Pressing the top half of the lower navigation button while the BIOS setup screen is open causes the cursor in the BIOS setup screen to move right. This is the same as if you had tapped Arrow Right on a keyboard.
	Pressing the bottom half of the lower navigation button while the BIOS setup screen is open causes the cursor in the BIOS setup screen to move left. This is the same as if you had tapped Arrow Left on a keyboard.

Table 1-5. Tertiary Functions of Application and Navigation Buttons

SECURITY FUNCTIONS OF APPLICATION BUTTONS

Five buttons are used when implementing security functions. Four of the buttons are used to enter the password, and the fifth is used as an Enter button. Instructions for using the security feature follow the table.

Button Icons	Security Icons	Security Purpose
Alt Ctl-Alt-Del Button	🔑	Security Enter Button
✉ EMail Button	1	Security Button 1
⧉ Orientation Button	2	Security Button 2
ESC Escape Button	3	Security Button 3
ENT Enter Button	4	Security Button 4

Table 1-6. Security Functions of Application Buttons

SETTING UP THE SECURITY PANEL

When you receive your Tablet PC, the security panel application is pre-installed without any passwords. The following sections provide detailed information on your security panel, how to set, change or remove passwords.

Numbered Buttons

Use these buttons to enter your password.*(Figure 1-6)*

Enter Button

After entering the button strokes, push this button to enter the password into the Tablet PC. *(Figure 1-6)*

PASSWORDS

The user and supervisor password may be set on this Tablet PC. A supervisor password is typically the same for all Tablet PC's and notebooks in a work group, office, or company to allow for system management. Individual computers in a group environment should not use a common password. A password consists of one to five button strokes plus the enter button. A valid stroke consists of pushing one or up to four buttons simultaneously.

The following are valid button strokes:

- Pushing [4] by itself
- Pushing [2] and [3] at the same time
- Pushing [1], [2], and [4] at the same time
- Pushing [1], [2], [3], and [4] at the same time

The following are valid passwords. The numbers within braces ({ }) are button strokes using more than one button.

- {[2]+[3]}, [1], [Enter]
- [4], [enter]
- {[1]+[3]}, {[2]+[3]+[4]}, [1], [4], [2], [Enter]

Setting Passwords

When shipped from the factory, no passwords are set. You have a choice of having no password or setting a supervisor and user password. You must set the supervisor password before the user password.

ℹ

- The purpose of supervisor password is to be able to bypass the user password in case the user password is forgotten. The supervisor password alone will not lock the system.
- You must set the supervisor **and** user passwords for the security panel to work.

Setting Supervisor Password

You must have set a supervisor password before setting any user passwords. The supervisor password can bypass the user password.

1. Go to the **Start** menu.
2. Click on **Run.**
3. Type in: `C:\Program Files\Fujitsu\Security Panel Application\Supervisor\FJSECS.EXE`, then press [Enter]
4. Follow the on-screen instructions to set the Supervisor password.

Setting User Password

1 Go to the **Start** menu.
2. Click on **All Programs**.
3. Click on **Security Panel Application** -> **Security Panel Application.**
4. Follow the on-screen instructions to set the user password.

You may change or remove the supervisor or user password by repeating the steps defined above.

USING YOUR SECURITY PANEL

The security lock feature is in effect both when the system resumes from Off, Standby, or Hibernation state. You always need to push the Security Panel buttons to input the user password. Your system will not begin the boot sequence until you enter your supervisor/user password.

From Off State

1. Turn on your system.
2. When the Security Indicator flashes, enter the password and press Enter button.

   For example, if the password is 22222, first press Button 2 five times and press the Enter button. The Tablet PC will boot to normal operation.

From Standby/Hibernation State

1. Press your Suspend/Resume button.
2. When the Security Indicator flashes, enter the password and press Enter button.

   The Tablet PC should resume normal operation.

Incorrect Password Entry

If an invalid supervisor or user password is entered three times in succession, the system will “beep” for about one minute. If a valid password is entered within a minute (while system beeps), the beeping will stop and the Tablet PC will resume normal operation. If no password is entered or an invalid password is entered while the system beeps, the system will return to its previous locked state (standby or off) and the Security Indicator will go off. To reactivate the Tablet PC after a password failure, you must press the Suspend/Resume button, then enter a correct password.

Remember the user password you specified on the Security Panel Application. If you forget the password you will not be able to use your computer. The supervisor password can override the user password.

PRECAUTIONS

Low Battery Operations

If your Tablet PC has a low battery, pushing the suspend/resume button does not unlock the Tablet PC. To resume normal operation, first attach a power supply to the system. Then you may unlock the Tablet PC.

UNINSTALLING THE SECURITY PANEL APPLICATION

You have two options when uninstalling the security panel application:

- Remove passwords and uninstall the security panel application software. This will disable all security features.
- Uninstall the security panel application with password still active. This will not allow any changes to the password.

Uninstalling the Security Panel Application Software

Remove passwords when User wants no password protection whatsoever and doesn’t want to give anybody the utility to set a password on their computer. In this case, if passwords (supervisor, user, or both) are set, the passwords must first be cleared BEFORE removing the application. To clear passwords, follow same procedure in SETTING PASSWORD CODES except this time, select REMOVE, enter current password then click **Next**. When asked to confirm select **Yes**.

Removing Security Panel Application with Passwords Still Active

Using this feature will not allow any changes to the password.

> Removing the applications does not remove the password. It simply removes the utility to change/add/remove passwords. To change your password you must reinstall the application.

User:

1. Go to Start -> Control Panel.
2. Open **Add or Remove Programs Properties** in the Control Panel.
3. Select the **Security Panel Application** in the list, and click **Change/Remove**.
4. When the Confirm File Deletion box appears, click **Yes**.

Supervisor:

1. Go to Start -> Control Panel.
2. Open **Add or Remove Programs Properties** in the Control Panel.
3. Select the **Security Panel Application for Supervisor** in the list, and click **Change/Remove**.
4. When the Confirm File Deletion box appears, click **Yes**.

Reinstalling the Security Panel Application

To reinstall supervisor or user security application, you will need your Drivers and Applications CD. The **Utilities\Security Panel Application** folder contains two separate folders: **Supervisor** and **User**. The setup files for supervisor and user security applications are contained in those folders.

1. Go to the **Utilities\Security Panel Application\Supervisor** folder on the CD and double-click the **setup.exe** file. The Installing Security Panel Application window will appear. Follow the instructions on the screen.
2. Go to the **Utilities\Security Panel Application\User** folder on the CD and double-click the **setup.exe** file. The Installing Security Panel Application window will appear. Follow the instructions on the screen.

Supervisor and user passwords can be set via Windows software using the FJSECS.exe and FJSECU.exe files, respectively. FJSECU.exe for the user password cannot run without first setting a supervisor password. You need to run FJSECS.exe first to set the supervisor password. Follow instructions under Setting Passwords on page 14.

If you forget both passwords, please contact Fujitsu Computer Systems Corporation Service and Support at 1-800-8Fujitsu (1-800-838-5487). Fujitsu Computer Systems Corporation charges a service fee for unlocking a password-restricted Tablet PC. When calling please have a valid credit card and provide proof of ownership. You will then be given instructions on where to ship your Tablet PC.

CONNECTORS AND PERIPHERAL INTERFACES

Connectors and peripheral interfaces on the Stylistic ST5000 Series Tablet PC allow the connection of a variety of devices. Specific locations are illustrated in Figures 1-2 through 1-5.

Table 1-7 provides a description of each peripheral connector on the Stylistic ST5000 Series Tablet PC. Each of the illustrated icons is either molded into or printed on the Tablet PC chassis.

Connector/ Peripheral	Tablet PC Icon	Purpose
DC input connector	⎓	Connect an external power source such as the AC adapter or auto/ airline adapter.
USB Port		Connect Universal Serial Bus 2.0 compliant devices to the Tablet PC.
PCMCIA Card slot	▭	Insert a Type I or Type II PC Card.
SD Card/ Memory Stick slot	SD	Insert a Secure Digital (SD) Card or a Memory Stick.
Microphone jack	🎤	Connect an external microphone. The internal microphone is disabled when you plug in an external microphone.
Headphone jack	🎧	Connect stereo headphones or powered external speakers. The internal speaker is disabled when you plug in external headphones or powered speakers.
IrDA/FIR port		An infrared transceiver built into the Tablet PC allows you to communicate with other devices that are compliant with the IrDA Standard Rev. 1.1. Effective range for infrared communication is about 3 feet, and within 15 degrees off center. A clear line-of-sight path must exist between the IrDA port on the Tablet PC and the IrDA transceiver on the other device.
Modem		Connect a telephone line to the optional internal modem using a standard RJ-11 telephone plug.
Tablet Dock port		Connect the Stylistic ST5000 Series Tablet Dock or other approved docking device. Refer to documentation accompanying the docking device for more information.

Connector/ Peripheral	Tablet PC Icon	Purpose
Infrared keyboard/ mouse port	⌨	An infrared receiver built into the Tablet PC allows you to communicate with a Fujitsu wireless infrared keyboard or mouse. The keyboard infrared port works optimally when it is placed between 10 to 30 cm (approximately 4 in. to 12 in.) from the keyboard infrared port (which is located on the bottom edge of the Tablet PC). Ensure there is a clear line-of-sight path between the infrared receiver on the Tablet PC and the infrared transmitter on the keyboard or mouse. Note that an infrared keyboard or mouse works best when the system is in landscape orientation.
Lock slot	🔒	The security slot allows you to secure the Tablet PC using compatible locking devices.
IEEE 1394 jack	1394	The IEEE 1394 jack allows you to connect IEEE 1394 (Firewire) devices such as digital video cameras and external hard drives to your Tablet PC.
Suspend/ Resume button	⏻	The Suspend/Resume/Power On button allows you to suspend Tablet PC activity without powering off, resume your Tablet PC from suspend mode, and power on the system when it has been shut down from Windows.
Page Up/ Page Down	⧉	The Page Up/Page Down button allows you to navigate quickly from page to page without scrolling.
Local Area Network (LAN)	🖧	The LAN (RJ-45) jack is used to connect the internal 10/100/1000* Base-T/Tx Ethernet to a Local Area Network (LAN) in your office or home, or broadband devices such as a cable modem, DSL, or satellite internet. *1000 Mbps, commonly referred to as Gigabit Ethernet.
Battery Release Latch	▶	The battery release latch allows you to remove the battery from your system for storage or replacement.
Wireless LAN/ Bluetooth On-Off Switch	⊚	The wireless LAN/Bluetooth switch allows you to turn power to the optional wireless LAN or Bluetooth devices on and off.
Fingerprint Swipe Sensor	⏏	The optional fingerprint swipe sensor allows you to avoid having to enter a user name and password every time you want to log into the system. This icon indicates the direction in which you should swipe your finger.

Table 1-7. Peripheral Connectors/Interfaces

2
Using Your Stylistic Tablet PC

Using the Stylistic ST5000 Series Tablet PC

This chapter covers the fundamental concepts, basic system operation and use, and system functions of the Stylistic ST5000 Series Tablet PC. You should familiarize yourself with this information before you attempt to operate the system.

Prior to using your system, be sure to **fully charge** the battery if you plan to run on battery power. Failure to do so may result in erratic performance.

SYSTEM STATES

Before you begin using the Stylistic ST5000 Series Tablet PC, review the different system states (or modes) that the system can use. Being familiar with these states will help you determine whether it is appropriate to turn on, resume, suspend, hibernate or shut down the system when you begin or end a session. System behavior for each system state is described briefly in the following, with each system state listed in decreasing order of power usage:

- **On state:** The system is running and the display screen is on.
- **Idle state:** Some system functions are regulated or turned off to conserve power. The display screen may be turned off. The system returns to the On state when pen activity or other input is detected.
- **Suspend-to-RAM mode (S3):** System operation is suspended. Most system functions are turned off to conserve power. Power to memory is on, maintaining data in programs that were running before system operation was suspended. The system does not respond to the pen or other input when in Suspend-to-RAM mode. Refer to the “Resuming System Operation” section later in this chapter for information on returning the system to the On state.
- **Hibernate mode (Save-to-Disk) (S4):** System operation is suspended. All system functions are turned off to conserve power. Active data in programs that were running before suspending system operation is stored on the hard disk drive. The system does not respond to the pen or other input. Refer to the “Resuming System Operation” section later in this chapter for information on returning the system to the On state.
- **Off state:** All system functions are turned off to conserve power. The system does not respond to the pen or other input. The system boots at the next system power-on.

The system consumes the same amount of power whether it is in Hibernate (Save-to-Disk) mode or the Off state.

Your system may be configured to enter some of these states automatically after a period of inactivity to conserve battery power.

When you use the Stylistic ST5000 Series Tablet PC, you can change the current system state in a number of ways, depending on the system’s current state. To determine the current system state, observe the Power icon in the Status display. Table 2-1 on page 22 gives the different system states represented by the Power icon and describes how you can change the system state from the current state.

Icon Appearance	Current State	To Change State[*]
⏻ Power icon displayed continuously	On State or Idle State	To enter the Off state, shut down the system using the Start menu on your system.
		To enter Suspend-to-RAM or Hibernate (Save-to-Disk)[†] state, suspend system operation using either a hardware or software suspend.
Power icon blinking	Suspend-to-RAM[†]	To enter the On state, resume system operation by pressing the Suspend/Resume button.
		To enter the Off state, resume system by pressing the Suspend/Resume button, then shut down your system.
Power icon not displayed	Off State, or, Hibernate (Save-to-Disk[†])	To enter the On state, start your system, or resume system operation by pressing the Suspend/Resume button.

Table 2-1 Changing System States

[*] Information in Table 2-1 on page 22 is supplied to help you understand which system states your system can enter from the current system state. Refer to the procedures on starting the system, shutting down the system, suspending system operation, and resuming system operation given later in this chapter.

[†] Your system may be configured to use either Suspend-to-RAM mode or Hibernate mode.

POWERING UP THE TABLET PC

Follow the procedure below to start the Stylistic ST5000 Series Tablet PC. Before you begin, confirm that the system is in the Off state. To do so, observe the Status display. If the Power icon is not visible in the Status display, the system is in Off state or in Hibernate (Save-to-Disk) mode and it is safe to perform this procedure. If the Power icon is visible (either blinking or on continuously), do not perform this procedure. See "System States" earlier in this chapter for details on modes represented by the Power icon.

1. Ensure that the battery in your Tablet PC is sufficiently charged, or connect an external power source such as the AC adapter or auto adapter to your Tablet PC.

2. Press the Power On/Suspend/Resume button to start the system.

After performing initialization, the system starts the operating system installed on the hard disk drive. Once the operating system is running, you can use the system.

SHUTTING DOWN THE SYSTEM

Follow these steps to shut down and turn off your system:

1. If system operation has been suspended, resume system operation. See "Resuming System Operation" later in this chapter for details.
2. Save your work and close all running programs.
3. Choose Shut Down from the Windows Start menu.
4. Carry out the Shut Down command.

The system is now in the Off state.

SUSPENDING SYSTEM OPERATION

The Tablet PC allows you to suspend the system operation without closing programs or exiting the operating system. Use this feature to conserve battery power when a system shutdown is not practical or when the battery needs to be changed.

> If you have set your system to turn power off from the Power Options utility in the Control Panel, the following procedure will not be possible, since pressing the button shuts the system down rather than suspending it. To change your power options, go to Start -> Settings -> Control Panel -> Power Options.

To suspend system operation:

1. Press the Suspend/Resume button, or carry out the Standby command from your operating system or power management program. (If your system is configured to suspend operation using Hibernate (Save-to-Disk) mode, which is explained later in this procedure, a message is displayed while data is saved to your hard disk.)

> ⚠ If you are replacing the battery, **wait until system operation is suspended and the power icon is flashing** before you remove the battery. Failure to do so could result in loss of your unsaved data. (Note that if the Resume On LAN function is enabled in the BIOS setup, you should **not** remove the battery unless the system is shut down. When Resume ON LAN is enabled, the bridge battery is disabled in order to optimize battery life.)

2. The Power icon either flashes (Suspend-to-RAM) or is not displayed (Hibernate) when system operation is suspended, depending on how your system is configured. At this point, programs that were running are stopped, active data is saved, and the system enters one of two different low-power states, or suspend modes, as explained in the following paragraphs.
3. Observe the Power icon in the Status display to determine which suspend mode your system is using.

- **Power icon is blinking:** *Suspend-to-RAM* mode.

  In this mode, active data is saved by maintaining power to RAM while most other system components are powered off. The Battery Gauge icon in the Status display indicates the battery charge level.

- **Power icon is not displayed:** *Hibernate (Save-to-Disk)* mode.

  In this mode, active data is stored on the hard disk drive and power usage is reduced to the same level used in the Off state. When the system is in *Hibernate* mode, the Battery Gauge icon is not visible in the Status display. In this mode, there is no danger of losing data if battery power is lost.

  If you have successfully performed this procedure, system operation is now suspended. Refer to “Resuming System Operation” later in this chapter to resume system operation. Also, note the following with regard to suspending system operation:

- You can remove the battery while the system is in Suspend-to-RAM or Hibernate modes in order to install a charged battery. To prevent losing unsaved data, wait until system operation has suspended before you remove the battery. Note that after you remove the battery, you have approximately five minutes to replace it with a new battery or to plug in a power supply before the bridge battery is depleted.
- Your system may be configured to suspend operation automatically after a period of inactivity.
- Your system may be configured to enter Hibernate mode automatically after a period of time in Suspend-to-RAM mode.
- The system uses a small amount of battery power when in Suspend-to-RAM mode. Eventually, the battery will become fully discharged.

> ℹ If you will not be using the system for an extended period, shut down the system rather than using Suspend-to-RAM mode.

- If the battery charge drops to a Low-Battery Warning level while the system is running, the system will beep periodically. If this occurs, suspend system operation, shut down the system, or attach an external power source, such as the AC adapter, to the Tablet PC.
- If the battery charge drops to a Critically Low level while the system is running, the system is forced into a Suspend-to-RAM or Hibernate mode. If this occurs, you must either install a charged battery, or connect an external power source such as the AC adapter before you can resume system operation. (If the charge drops to a Critically Low level while the system is *in* Suspend-to-RAM mode, the system stays in that mode until power is restored or totally dissipated.)
- Suspending system operation interrupts data communications; therefore, some programs may block the system from suspending to prevent an interruption.
- The suspend action of the Suspend/Resume button may be disabled to prevent accidental interruption. If this is the case, pressing the Suspend/Resume button will not suspend system operation as described here. (In this case, suspend mode can only be achieved using the system software). Contact your local help desk or reseller if your system configuration is not suitable.
- If your system is equipped with a PC Card that allows you to connect to a wired or wireless network, you may be logged off the network after a period of inactivity while system operation is suspended. Contact your network administrator or help desk, or call Fujitsu Service and Support at 1-800-8Fujitsu (1-800-838-5487) for details on your network log-off parameters.

RESUMING SYSTEM OPERATION

To resume operation from either Suspend-to-RAM or Hibernate modes, press the Suspend/Resume button.

- **From Suspend-to-RAM mode**
  Status lights indicate that the system state is changing. It may take up to a minute before the system returns to the On state and system operation resumes. Note that the display turns on shortly before the pen becomes active due to the power-up sequences observed by the system.
- **From Hibernate (Save-to-Disk) mode**
  Active data is read from the hard disk drive, and the system returns to the On state after a short time.

Note that power to several system components must be restored before system operation resumes. Allow sufficient time for system operation to resume before attempting to use the system. If your system uses Hibernate mode, it will take longer to resume operation as compared to using Suspend-to-RAM mode. Time is needed to read data from the hard disk drive.

Use the system as you normally would once system operation resumes.

All programs resume at the point where execution stopped when system operation was suspended.

ADJUSTING THE DISPLAY BRIGHTNESS

There are four ways to adjust your display's brightness:

Depending upon whether you are running your system on battery or AC power, the default screen brightness settings will be different. The screen brightness default for running on battery is lower than that on AC power in order to optimize battery life.

- Click the Tablet icon in the system tray at the bottom right of the screen. (When the cursor is on top of the icon, a message stating "Change tablet and pen settings" is displayed.) When the Tablet and Pen Settings window appears, select the Display tab, and move the Screen Brightness slider to change the brightness.
- Click Start -> Control Panel -> Tablet and Pen Settings. Select the Display tab, and move the Screen Brightness slider to change the brightness.
- Click the Fujitsu Menu icon in the system tray at the bottom right of the screen. (When the cursor is on top of the icon, a message stating "Fujitsu Menu..." is displayed.) Select Tablet and Pen Settings and select the Display tab. Move the Screen Brightness slider to change the brightness.
- Press the Fn key twice to invoke the Fujitsu menu and select Tablet and Pen Settings.

USING THE PEN

You can use the Stylistic ST5000 Series pen to generate and create electronic "ink", to select items, and to navigate through programs on the Tablet PC. Programs that support handwriting recognition also allow you to write characters directly on the screen with the pen. You can also use the pen as a drawing tool.

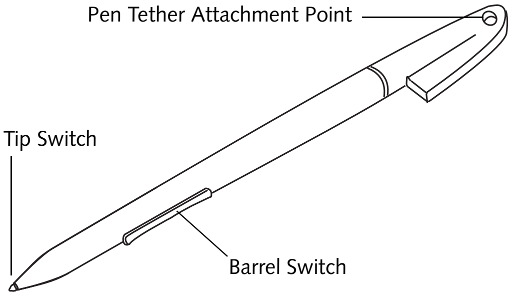


Figure 2-1. Stylistic ST5000 Series Pen

The Stylistic ST5000 pen is a sophisticated, high-quality electronic instrument that can be damaged if used improperly. Treat the pen as you would any precision device. The following list contains guidelines for proper pen handling:

- Do not gesture with the pen, use it as a pointer, or tap it on surfaces other than the Tablet PC screen.
- Do not try to turn the thumb grip on the pen; it is designed for inserting and removing the pen from the pen holder and for attaching a pen tether.
- Never store the pen with the tip bearing the weight of the pen (e.g., sitting tip down in a pencil cup). Storing the pen tip down could distort the internal mechanism over a period of time (especially in higher temperatures), causing the tip to act as if it is always depressed. To avoid damage, the pen should be stored in the pen holder when not in use.

The screen reacts when the pen tip is approximately 1/8 inch (3-5mm) from the screen. The pen has three switches: a tip switch and a barrel button toggle switch with switches at both ends. When activated, the tip switch corresponds to the left mouse button, and the front toggle (closest to the pen tip) barrel button switch, when used in combination with the tip switch, corresponds to the right mouse button. The rear toggle of the barrel button switch acts as an electronic ink "eraser" when it is so configured in the Control Panel. Note that the erasing feature is application-dependent.

⚠

- Ensure that a screen protector is installed on the Tablet PC screen before you use the pen. The warranty does not cover a scratched screen.
- Use **only** the pen provided with your Tablet PC. Do not use substitutes that were not designed for the Stylistic ST5000 Series Tablet PC.

Here are some hints that may help you use the pen more effectively:

- **To activate the tip switch,** tap or hold the pen tip against the screen.
- **To activate the barrel button switch,** press and hold the end of the button you wish to use (front toggle is the right mouse button switch; the rear toggle acts as an electronic "eraser".
- **To move the cursor,** hold the pen tip within 1/8 inch (3 - 5mm) from the screen and move the pen.
- **To start a program,** double-tap the pen tip (tap the pen tip twice rapidly) on the program icon as you would double-click a mouse.
- **To select an object,** tap the pen tip on the object once.
- **To "double-click" an object,** tap twice on the object quickly.
- **To move, or "drag", an object on the screen,** place the pen tip directly over the object, then as you hold the pen tip against the screen, move the pen.

CALIBRATING THE PEN

For information about calibrating your pen, refer to the literature that came with the operating system.

INSTALLING A PEN TETHER

To prevent dropping or losing your pen, you should attach it to your system using the pen tether that is included with the system.

To attach the pen tether to your Tablet PC, perform the following steps:

1. Attach the end of the pen tether with the smaller loop to your pen. Do do so, push the end of the tether through the hole in the pen, then thread the opposite end of the tether through the loop. (*See Figure 2-2.*)

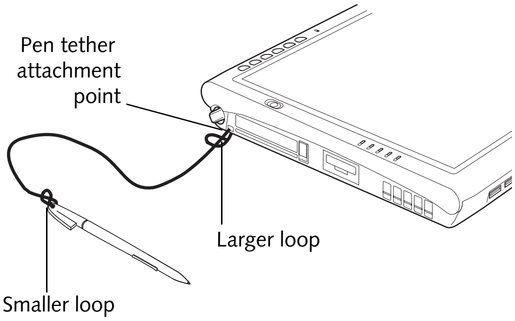


Figure 2-2. Installing a Pen Tether

2. Attach the end of the pen tether with the larger loop to the attachment point on your pen tablet. To do so, insert the end of the pen tether through the attachment point, then feed the pen through the large loop in the tether.

REPLACING THE PEN TIP

With use, the pen tip may become worn or may pick up foreign particles that can scratch the screen. A damaged or worn tip may not move freely, causing unpredictable results when using the pen. If your pen exhibits these problems, you should replace the pen tip. To do so, use the pen tip removal tool included with your pen.

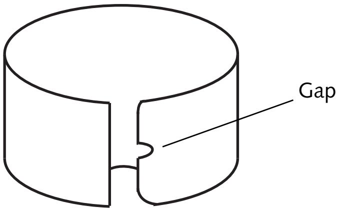


Figure 2-3. Tip Removal Tool

To remove the tip, position the tip in the gap between the two ends of the tool. Pinch the tool together so the tip is firmly clasped, then pull it from the barrel. If the tip is worn or damaged, discard it.

To replace the tip, retrieve one of the new tips that accompanied your pen. Insert the flat end of the tip into the barrel and push it in firmly until it is seated.

If you need more tips, they can be ordered from the Fujitsu Web site at: us.fujitsu.com/computers.

CHARGING THE BATTERY

The Stylistic ST5000 Series battery can be charged while it is installed in the Tablet PC.

To do so:

1. Connect a DC power source, such as the AC adapter, to the DC input connector on the Tablet PC. The DC Input icon appears in the Status display. If the battery

charge is below 90%, the battery begins charging and the Charging icon appears in the Status display. If the battery charge is 90% or higher *when you connect* DC power, the battery will not charge, preventing battery overcharging.

2. Look at the Battery Gauge icon in the Status display to determine the percent of charge in the battery. See "Status Display" in Chapter 1 of this manual for a description of the Battery Gauge icon.

As long as DC power *remains connected* to the Tablet PC, the charging process continues until the battery charge reaches 100%.

Also note the following with respect to charging the battery:

- You can use the system, suspend system operation, or shut down and turn off the system without interrupting the charging process; however, using the system while the battery is charging will cause the battery to charge at a slower rate.
- As noted in the procedure above, the system will not begin charging the battery if the battery charge level is 90% or higher when the system is *initially connected* to external DC power. (This prevents the battery from being overcharged.)
- The battery uses Lithium ion battery cells which have no "memory effect." You do not need to discharge the battery before you begin charging.

REMOVING AND INSTALLING THE BATTERY

The battery can be removed from the Tablet PC and swapped with a charged battery. The battery can then be charged in an external charger if one is available. To remove the battery from the Tablet PC:

1. Choose one of the following:
   - If a charged battery is available, you can suspend system operation. A built-in "bridge" battery will maintain the system in Suspend-to-RAM mode for about 5 minutes while the battery is removed; this allows time for replacement with a charged battery.
   - If a charged battery is not available, save your work and close all running programs, then shut down the system or Hibernate (Save-to-Disk).
   - Plug in an external DC power source.
2. Slide the battery release latch in the direction indicated. *(See Figure 2-4 on page 26 for location).*
3. Pull the battery away from the system, as shown in the illustration and remove the battery from the Tablet PC.

If you are using an external battery charger, refer to the instructions provided with the battery charger.

> Under Federal, state, or local law, it may be illegal to dispose of batteries by putting them in the trash. Be sure to dispose of batteries in accordance with local government regulations.

To install the battery:

1. Orient the battery with the slides in the empty battery tray. Slide the battery into the tray and press it firmly until it is seated. When it is properly seated, the battery release latch should return to position and lock the battery.

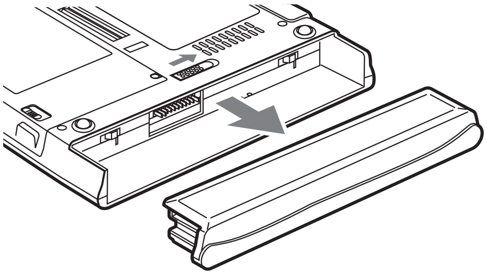


Figure 2-4. Removing the Battery

Once the battery is installed, you can resume system operation or start and use your system normally.

TIPS FOR CONSERVING BATTERY POWER

You can extend the charge life of your battery by conserving battery power. (Your results may vary depending on your application and how the system is configured.) Here are some suggestions to help you conserve battery power:

- Use an external power source such as the AC adapter whenever the system is docked.
- Suspend system operation if you know that you won't be using the system for a while.
- Shut down the system if you won't be using the system for an extended period of time.
- Switch the wireless LAN switch Off when wireless LAN functionality in not needed (applicable only for systems with optional wireless LAN).
- Use power management (available on the desktop) to help you conserve power automatically.
- Reduce the brightness of the LCD.
- Battery life is dependent upon the operating system, power settings, and applications in use.

Operation of the Bridge Battery

When installed in the Tablet PC, the battery provides power to some system components—even when the system is in the Off state. When the battery is removed, power is supplied to these components by a "bridge" battery that is built into the Tablet PC.

The bridge battery is not designed for long-term operation. To maintain the bridge battery properly, observe the following measures:

- The bridge battery function is disabled if Wake On LAN is enabled in the BIOS.
- The system arrives with the bridge battery in a discharged state. Be sure to charge it sufficiently before relying upon it to support the system in the event of battery removal.

- To prevent draining the bridge battery, always store the system with a charged battery installed.
- If the bridge battery becomes drained, it takes approximately 8 hours for it to be fully recharged.
- The bridge battery charges when the AC Adapter is connected and the system is in On or Off states or Suspend mode. It charges from the battery only when the system is in the On state.

MODEM CONNECTION

The internal 56 Kbps LAN/modem module installed in the Stylistic ST5000 Series Tablet PC has actual maximum transfer rates of 53 Kbps (receive), 33.6 Kbps (send), and 14.4 Kbps (fax). Download rates are limited to 53 Kbps in the United States due to FCC restrictions.

The Stylistic ST5000 Series Tablet PC is designed to accept a standard RJ-11 telephone plug. Connect the plug to the modem jack located on the left-hand side of the Tablet PC *(See Figure 1-5 on page 6 for location)*. The telephone plug can be inserted whether or not the Tablet PC has power applied.

If you need assistance configuring the Stylistic ST5000 Series Tablet PC modem or LAN, contact your local help desk or reseller.

MEMORY STICK/SD CARD SLOT

Your Tablet PC supports Memory Stick and SD flash memory cards on which you can store and transfer data to and from a variety of digital devices. These cards use flash memory architecture, which means they don't need a power source to retain data.

Note that MagicGate functions are not supported by this slot.

Memory Stick is a flash memory technology developed by Sony Electronics. Memory Stick allows you to record, transfer and share digital content, such as digital pictures, movies, music, voice, and computer data and applications.

Secure Digital (SD) Cards are very similar to Memory Sticks, but they are shorter. Like the Memory Stick, SD Cards allow portable storage among a variety of devices, such as cell phones, GPS systems, digital cameras, and PDAs. SD Cards transfer data quickly, with low battery consumption. Like the memory stick, it uses flash memory architecture.

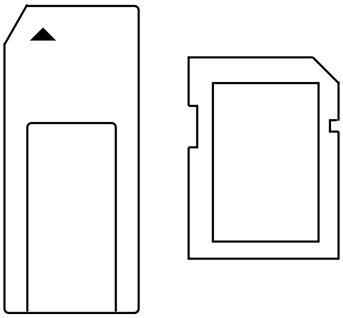


Figure 2-5. Memory Stick and Secure Digital Card

Inserting Memory Stick/SD Cards

Memory Sticks and SD Cards are inserted in the Memory Stick/SD Card slot *(Figure 1-4)*. To insert a Memory Stick or SD Card, follow these steps:

- Inserting or removing a Memory Stick or SD Card during your system's shutdown or bootup process may damage the card and/or your computer.
- Do not insert a card into a slot if there is water or any other substance on the card as you may permanently damage the card, your Tablet PC, or both.

1. See your Memory Stick or SD Card manual for instructions on the insertion of your card. Some cards may require that your system is off while inserting them.
2. Make sure there is no card currently in the slot. If there is, see Removing a Memory Stick/SD Card.
3. Insert your card into the slot with the product label facing up.
4. Push the card firmly into the slot until it is seated in the connector.

Removing A Memory Stick/SD Card

To remove a Memory Stick/SD Card, follow these steps:

See your Memory Stick or SD Card manual for specific instructions on the removal of your card. Some cards may require your computer to be in Suspend Mode or Off while removing them.

Push the Memory Stick or SD Card in until it unlatches. It will then eject from the slot for removal

PC CARD SLOT

The Stylistic ST5000 Series Tablet PC Card slot allows you to insert a Type I or Type II PCMCIA Card.

Inserting a PC Card

To insert a PC card, position the side with the arrow facing up (i.e., when looking at the tablet's display side, the arrow on the card should be visible.) Slide the card into the PC Card slot, and press it firmly to ensure proper seating. *(See Figure 2-6 for location)*

If you need assistance inserting a PC Card in the Stylistic ST5000 Series Tablet PC, contact your corporate help desk or reseller.

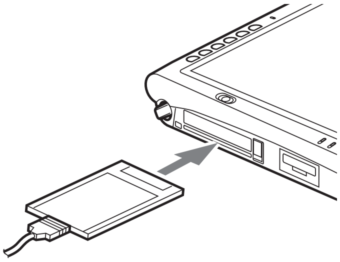


Figure 2-6. Inserting a PC Card

Removing a PC Card

To remove a PC Card, first click the Safely Remove Hardware icon in the system tray in the bottom right-hand corner of the display. Select PC Card from the list, and click [Stop].

Press the PC Card eject button so that it pops out. Once the button has popped out, press it firmly to eject the card. *(See Figure 2-7 for location)*

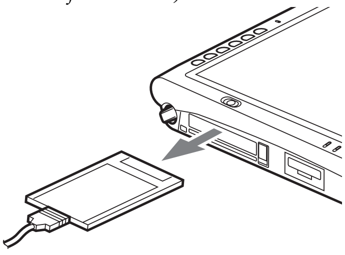


Figure 2-7. Removing a PC Card

REMOVING AND INSTALLING MEMORY MODULES

There are two DIMM slots in your Tablet PC. 256 MB, 512 MB, and 1 GB modules are available, so you can install a combination of up to 2 GB in the system.

DIMM replacement should be performed at a static-free workstation. Do not touch connector pins, circuit boards, or other circuit components on the drive or Tablet PC. Electrostatic discharge caused by doing so can damage sensitive components.

Installing a Memory Module

To install a DIMM module in the Tablet PC:

1. Ensure that the Tablet PC is off. To do so, carry out the Shut Down command in the Start menu. (Do not attempt to remove or install a DIMM module when the system is in Suspend mode or running.)
2. Remove the two screws from the cover plate on the back of the Tablet PC and remove the cover plate as shown in Figure 2-8.

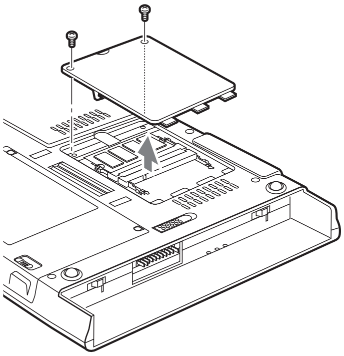


Figure 2-8. Accessing the Memory Slot

3. Insert the DIMM module in the socket at an angle and push it down until it locks into place as shown in Figure 2-9. Note that the DIMM module is keyed to prevent it from being inserted backwards.

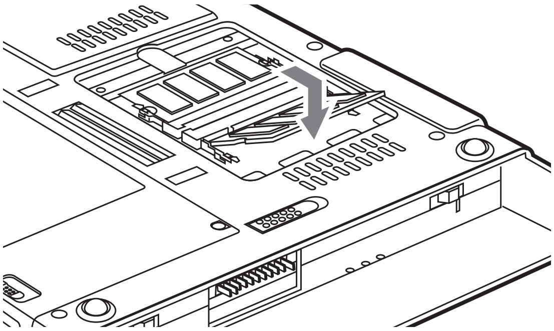


Figure 2-9. Installing a DIMM Module

4. Reinstall the cover and screws that you removed in step 2.

5. Confirm that the DIMM module is recognized by the system. To do so, run BIOS Setup. The size of the DIMM module should be displayed in the Info menu in BIOS Setup.

The DIMM module is installed in the Tablet PC and you can now use the system.

Removing a Memory Module

To remove a DIMM module:

1. Ensure that the Tablet PC is off. To do so, carry out the Shut Down command in the Start menu. (Do not attempt to remove or install a DIMM module when the system is in Suspend mode or running.)

2. Remove the screws from the cover plate on the back of the Tablet PC and remove the cover plate as shown in Figure 2-8.

3. Spread the fingers on the socket that lock the DIMM module in place until the DIMM module is loose.

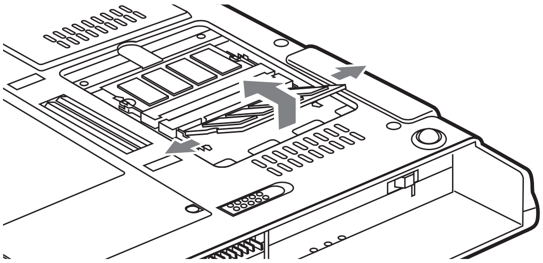


Figure 2-10. Removing a DIMM Module

4. Remove the DIMM module from the socket.

The DIMM module is now removed from the Tablet PC. See "Installing a Memory Module" to install a new DIMM module.

3
Care and Maintenance

Care and Maintenance

This chapter gives you pointers on how to care for and maintain your Stylistic ST5000 Series Tablet PC.

CARING FOR YOUR TABLET PC

Please note the following information regarding proper treatment of your Tablet PC:

- Your Tablet PC is a durable but sensitive electronic device. Treat it with respect and care.
- Make a habit of transporting the system in a suitable carrying case.
- Do not attempt to service the computer yourself. Always follow installation and operation instructions closely.
- If you accidentally spill liquid on your Tablet PC:
  1. Turn it off.
  2. Position it so that the liquid can run out.
  3. Let it dry out for 24 hours, or longer if needed.
  4. If your Tablet PC will not boot up after it has dried out, call your support representative.
- Do not use your Tablet PC in a wet environment (near a bathtub, swimming pool).
- Always use the AC adapter and batteries that are approved for your system.
- Avoid exposure to sand, dust and other environmental hazards.
- Do not expose your Tablet PC to direct sunlight for long periods of time as excessive temperatures may damage your system.
- Do not put heavy or sharp objects on the computer.
- Do not carry your system in a bag or briefcase while it is running; doing so could result in overheating or hard disk drive problems.
- If you are carrying your system in a briefcase, or any other carrying case, make sure that there are no objects in the case pressing on the display.
- Do not drop your Tablet PC or touch the screen with any sharp objects.

PROTECTING THE DISPLAY SCREEN

The Stylistic ST5000 Series Tablet PC is designed to provide you with years of service. Using a screen protector will help ensure the screen remains as clear as possible. When installed, the screen protector becomes a durable, replaceable writing surface that protects the display screen from abrasion.

To obtain additional screen protectors, use Fujitsu part number FPCSP08AP (6-pack) when ordering. Additional information about installation is included with the screen protectors.

⚠ During normal use of the Tablet PC, small particles from the environment can become embedded in the pen tip and scratch the screen. To prevent scratching the screen, ensure that a screen protector is installed before using your Tablet PC. The warranty does not cover a scratched screen.

To install a new screen protector on your Tablet PC:

1. If a screen protector is already installed on the display screen, remove it before installing the new screen protector.

   The screen protector is held onto the display screen surface by a thin strip of adhesive around the edges. A notch in one corner of the screen protector allows you to slide your fingernail under the screen protector for easy removal.

2. Clean the display by wiping the screen gently using a soft cotton cloth dampened with isopropyl alcohol. Ensure that all residue has been removed from the screen before applying a new screen protector. Remove the protective coating from the adhesive side of the screen protector first, as shown in Figure 3-1.

⚠
- The Stylistic ST5000 Series Tablet PC is **not waterproof**. Do not pour liquids on the system or wash it with a heavily soaked cloth.
- Do not place items on the top of the display, or damage may occur.

.

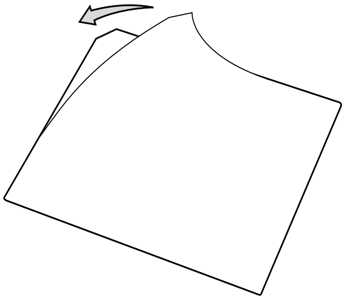


Figure 3-1. Removing the Protective Sheet

3. Apply the screen protector to the display screen surface. When doing so, orient the screen protector with the adhesive side of the screen protector facing the display screen and the notched corner of the screen protector oriented as shown in Figure 3-2.

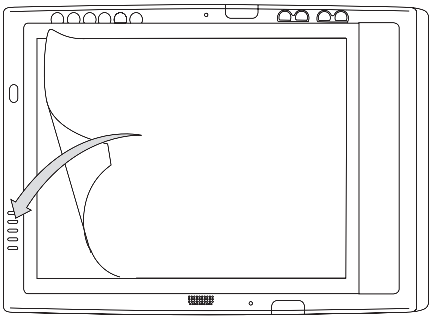


Figure 3-2. Installing the screen protector

4. Apply pressure to the screen protector with your finger using a continuous wiping motion along the edges. The adhesive sets completely within 48 hours. To ensure a good seal between the screen protector and the display, do not lift the screen protector from the display once it has been applied.

5. Remove the protective plastic cover from the face of the screen protector, as shown in Figure 3-3.

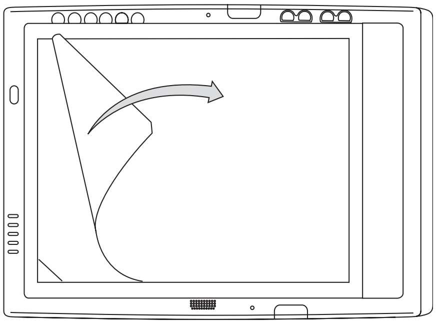


Figure 3-3. Removing the protective cover

6. Clean any residue left behind by the protective coating from the exposed surface of the screen protector by wiping gently with a soft cotton cloth dampened with isopropyl alcohol. Wipe the screen protector with a soft dry cloth to remove any low-tack adhesive; this will help prevent the pen tip from squeaking.

STORING THE TABLET PC

Store the Stylistic ST5000 Series Tablet PC in the Off state with a fully charged battery installed. You can store the Tablet PC in the Off state for about 30 days with a fully charged battery installed. After this period, the battery should be recharged or replaced with a charged battery.

If you intend to store the Tablet PC for a longer period of time, the small battery that maintains system time may need to be replaced. Replacement of the clock battery should only be performed by authorized technicians.

AVOIDING OVERHEATING

⚠ Do not expose your Tablet PC to direct sunlight for extended periods of time. High temperatures could damage your tablet.

The Tablet PC monitors its internal temperature. As the internal temperature approaches the tolerable limits of heat-sensitive components, system functions are automatically limited or turned off to prevent damage.

To protect your notebook from damage and to optimize performance, **keep all air all vents unobstructed**, **clean, and clear of debris**. This may require periodic cleaning, depending upon the system environment.

Do not operate the notebook in areas where the air vents can be obstructed, such as in tight enclosures or on soft surfaces like a bed or cushion.

CLEANING THE DISPLAY SCREEN

To clean the Tablet PC display screen, wipe the screen surface gently using a soft cotton cloth slightly dampened with water or isopropyl alcohol.

⚠ The Tablet PC is **not waterproof**. Do not pour liquids on the Tablet PC or wash it with a heavily soaked cloth.

TROUBLESHOOTING

Solutions to some common problems are described in the following sections. If you are experiencing a problem with your Tablet PC that you cannot solve by taking the actions described, contact your local help desk or reseller, or call Fujitsu Service and Support at 1-800-8Fujitsu (1-800-838-5487) for further assistance.

System Will Not Resume Operation

If the system will not resume operation after system operation has been suspended, check the following:

- The battery may either be defective, or discharged to a critically low level. When the battery reaches a critically low level, the system is forced into Suspend-to-RAM mode to avoid a total system power failure. To correct this problem, either connect an external power supply (such as the AC adapter), or install a charged battery in the Tablet PC.
- The system may be at the critical thermal limit. To avoid damage to heat-sensitive components, the system enters Suspend-to-RAM mode when it gets too hot. System operation cannot be resumed until the Tablet PC cools off to a tolerable temperature. Move the Tablet PC to a cooler location.

Display Screen Blank or Difficult to Read

If the display screen on your Tablet PC appears blank or is unreadable, confirm that the system is running (the Power icon is displayed continuously on the Status display), and check the following:

- The system brightness may be set too low, causing the screen to appear too dark. To change system brightness, press the **Fn** button twice to open the Fujitsu menu. Brightness can be adjusted from the menu.
- The video timeout may have expired. Tap on the display screen to reactivate the display. Note that this is a normal, power-saving feature.

Cursor Is Not Tracking Pen

If the cursor on the screen appears to be misaligned with the pen or is not accurately tracking the pen, calibrate the pen. See "Calibrating the Pen" on page 25 for more information.

Infrared Data Transfer Is Not Working

If you are experiencing problems transferring data over the system's infrared interface, note the following:

- Can the IrDA port on the Tablet PC "see" the IrDA port on the other device? A direct line-of-sight path must exist between the IrDA port on the Tablet PC and the IrDA port on the other device.
- The distance between the two devices must not be more than 3 feet.
- The viewing angle from the IrDA port on the Tablet PC must not be more than 15 degrees from a center line between the IrDA port on the Tablet PC and the IrDA port on the other device.
- The device with which you are trying to communicate must be compliant with the IrDA Standard Revision 1.1 (or 1.0).
- It may be necessary for both computers to be using the same network connection protocols.

Tablet PC is Not Responding to the Pen

If the Tablet PC does not respond to the pen, connect an external keyboard to the system to see if it responds to keyboard commands. If the system doesn't respond to a keyboard, the application or system may have crashed, and it may be necessary to reboot the system. If the system responds to a keyboard but not to a pen, contact your local help desk or reseller, or call Fujitsu Service and Support at 1-800-8Fujitsu (1-800-838-5487) for further assistance.

Speaker/Headphone Volume Too Low

If the audio volume on your Tablet PC speaker or external headphones is too low, check the following:

- Ensure the speaker (or headphone output if using headphones) is enabled. To do so, open the Control Panel and double-click on the Sounds and Audio Devices icon. Select the proper tab, and increase the volume using the slider bar. (If you aren't getting any sound, uncheck the Mute box if it is checked.)
- Press the **Fn** button twice to open the Fujitsu menu. Volume can be adjusted from the menu.
- Ensure the mute box in the system volume control (accessible from the system tray) is not set.
- Ensure any volume control in your audio software is set to an audible level.

Configuring Peripheral Interfaces

Certain peripheral devices can be disabled during the BIOS Setup. If the peripheral interface you want to use does not appear to be working with your peripheral device, ensure that it is enabled in the BIOS. Contact your local help desk or reseller, or call Fujitsu Service and Support at 1-800-8Fujitsu (1-800-838-5487) if you need assistance using BIOS Setup.

RESTORING THE PRE-INSTALLED SOFTWARE

The Drivers and Applications Restore (DAR) DVD contains sets of device drivers and Fujitsu utilities (in specific directories) that are unique to your computer configuration for use as documented below.

If you have access to the internet, visit the Fujitsu Support web site at: http://www.computers.us.fujitsu.com/support to check for the most current information, drivers and hints on how to perform recovery and system updates.

Re-Installing Individual Drivers and Applications

The Drivers and Applications CD can be used to selectively re-install drivers and/or applications that may have been un-installed or corrupted.

There may be certain free third-party applications pre-installed on your system that are not on the DAR CD. The latest versions of the applications can be downloaded from the third-party's website.

To re-install drivers and/or applications:

1. Boot up the system and insert the DAR CD after Windows has started. A Fujitsu Installer screen is displayed after the CD is inserted.
2. After reading the License Agreement, click [I agree].

3. A window will appear containing a list of applications, drivers, and utilities that you can install from the Drivers and Applications CD.

> The components listed are color-coded in terms of their install status. Blue indicates that the component can be installed. Green indicates that the component needs to be installed separately. Grey indicates a component that is already installed; grey items can be reinstalled, but prior to installation you will receive a reminder that the component is already installed.

4. In the list, check off all the components you want to install. If you want to install all components, click [Select All]. Clicking [Select All] will select all of the blue-coded components; you must select grey and green components separately.
5. Once you have selected the components you wish to install, click [Install Selected Subsystems]; the components will be installed.
6. After the components are installed, click [OK], then click [Yes] when asked if you want to reboot the system.

RESTORING THE FACTORY IMAGE

> The Restore Disc only restores the primary hard disk drive. If you have an optional second hard disk drive installed, **it will not be restored** using these utilities.

The Restore Disc that came with your system contains two utilities:

- The **Recovery** utility allows you to restore the original contents of the C: drive.
- The **Hard Disk Data Delete** utility on this disc is used to delete all data on your hard disk and prevent it from being reused. Do not use the Hard Disk Data Delete utility unless you are absolutely certain that you want to erase your entire hard disk, including all partitions.

> - The use of this disc requires that you have a device capable of reading DVDs attached to your system. If you do not have a built-in DVD player, you will need to attach an external player. For more information on available external devices, visit our Web site at: **us.fujitsu.com/computers**.
> - This disc can only be used with the system with which it was purchased.

BOOT Priority Change

Before restoring an image, you must first verify that your system is set up to boot from the DVD drive. To verify/change the boot-up priority (rather than booting-up from the hard drive or an external floppy disk drive), perform the following steps:

1. Start your system and press the [F2] key when the Fujitsu logo appears. You will enter the BIOS Setup Utility.
2. Using the arrow keys, go to the Boot menu.
3. Arrow down to the Boot Device Priority submenu. Press [Enter].
4. If "Optical Media Drive" or "CD-ROM Drive" is not at the top of the list, arrow down to the drive in the list, and press the space bar (or the + key) to move it to the top of the list. (The system attempts to boot from the devices in the order in which they are listed.). Note that the BIOS for some systems will indicate "CD-ROM Drive", even when a DVD drive is connected.
5. If you have an *external* DVD drive connected, proceed to the next step; otherwise, proceed to step 7.
6. If you have an external DVD drive connected:
   - Select the Advanced menu in the BIOS window.
   - Scroll down to the USB Features submenu and press the Enter key to open it.
   - If Legacy USB Support is disabled, press the space bar to enable it.
   - Scroll down to SCSI SubClass Support and press the space bar to enable it.
7. Press [F10], then click on [Yes] to exit the BIOS Setup Utility and return to the boot process.

After you have changed the boot priority, you can restore a backup image when you are booting up.

Procedure

1. Turn on the power to your system.
2. Ensure that you have a device that can read DVDs either installed in your system or attached externally to it.
3. Insert the Restore Disc into the drive tray.
4. Reboot your system.
5. After the system reboots, follow the instructions that appear to either restore your system image or erase all data from your hard disk.

AUTOMATICALLY DOWNLOADING DRIVER UPDATES

Your system has a convenient tool called the Fujitsu Driver Update (FDU) utility. With FDU, you can choose to automatically or manually go to the Fujitsu site to check for new updates for your system.

The FDU icon should appear in the system tray at the bottom right of your screen (roll the cursor over the icons to find the correct one). If the FDU icon does not appear in the system tray, it can be started by going to [Start] -> All Programs, and clicking on Fujitsu Driver Update; this will create the icon automatically.

To invoke the FDU menu, right-click on the FDU icon. The menu contains the following items:

- **Check for updates now**
  Allows for manual driver update search. The first time it is used, you are prompted to agree to a user agreement. After clicking on the icon, the FDU automatically connects with the Fujitsu site to check for updates and downloads them. While downloading, the icon has a red bar through it, indicating that it cannot be used while the download is in process. When the update is complete, a message appears informing you of the fact.
- **Enable Automatic Update Notifications**
  Automatically searches for new updates on a regular basis (approximately every 3 days).
- **Show update history**
  Brings up a screen that displays a history of updates that have been made via the FDU.
- **About Fujitsu Driver Update**
  Displays the FDU version number and copyright information
- **Fujitsu Driver Update Readme**
  Displays the FDU readme.

4
Specifications

Stylistic ST5000 Series Hardware Specifications

The following table provides general hardware specifications of the Stylistic ST5000 Series Tablet PC by category.

Stylistic ST5000 Specifications	
Processing Specifications	
CPU	Intel® Pentium® M Processor ULV 753*
Chip set	Intel 915GM - 400 MHz FSB
Processor Speed	1.2 GHz*
Memory/Storage Specifications	
Main RAM	• 2 DIMM slots available • 200-pin SO DIMM modules • DDR2 400 MHz • 256 MB, 512 MB, and 1 GB module configurations available, with a system maximum of 2 GB.
L1 cache (CPU)	32 KB on-die
L2 cache	2 MB on-die
BIOS ROM	1 MB (FWH)
Hard disk drive	• 2.5″ HDD • Minimum 40 GB IDE HDD* • ATA 100 • 5400 rpm • Shock-mounted
Display Specifications Depending on the configuration of your system, it has either a 12.1" transmissive or a 10.4" reflective display	
12.1" Display	• Transmissive Color LCD • Active Digitizer • 16-bit color • 12.1″ TFT XGA (1024 x 768), 16M colors • Brightness: 8 levels • Viewing Angle: Horizontal: 80 degrees (max.) Vertical: 80 degrees (max.) • Contrast Ratio: Typ. 250, Min. 100

* The specifications for your particular model may vary. To determine the specifications for your system, please visit our Web site at: us.fujitsu.com/computers.

Stylistic ST5000 Specifications (Continued)	
10.4" Display	• Reflective Color LCD • Active Digitizer • Outdoor-viewable • 16-bit color • 10.4″ TFT XGA (1024 x 768), 16M colors • Brightness: 8 levels
VRAM	Up to 128 MB of shared memory using Unified Memory Architecture (UMA). Dynamically responds to application requirements and allocates the proper amount of memory for optimal graphics and performance.
Physical Specifications	

Dimensions	12.1" Display (Active Digitizer):
	8.66" w x 12.77" d x 0.82"-0.88" h (220 mm x 324.4 mm x 20.9-22.3 mm)
	10.4" Display (Reflective Digitizer):
	8.66" x 12.76" x 0.91"-0.98" (220 mm x 324.1 mm x 23.0-24.9 mm)

Weight	3.5 lbs. (1.59 Kg) (with battery)
Interface Specifications	
Card Slots	• PCMCIA: One Type I or Type II, PCMCIA CardBus version 3.0 • Secure Digital (SD)/ Memory Stick slot • Smart Card slot
Integrated Interfaces	• Modem (RJ-11) • LAN (RJ-45) • IEEE 1394 (S400 4-pin) • USB 2.0 (Qty. 2) • DC-In • IrDA • 15-pin D-SUB connector for external VGA monitor • Docking connector
Infrared	IrDA version 1.1 (FIR, 4Mbps)
Keyboard/ Mouse support	Keyboard/Mouse IR Port (Qty. 2)

Stylistic ST5000 Specifications (Continued)	
Wireless LAN	Your system may have one of the two following Wireless LAN devices installed: • Integrated Intel PRO/Wireless 2915ABG Network Connections (802.11a+b/g) • Integrated Atheros Super AG Wireless LAN (802.11a/b/g)
Audio	• Sigmatel STAC9753A codec • Internal mono microphone and speaker • Dual microphones (12.1" model only) • Stereo headphone jacks
User Controls	• Application Buttons, each with primary, secondary, tertiary, and security functions • Fingerprint swipe sensor for biometric security (12.1" model only) • Power On/Suspend/Resume button • Emergency Shutoff Button (Power Off button) • Two Navigation buttons
Status Indicators (LEDs)	• Power • Charge/DC-In • Battery level • HDD • Security
Power Specifications	
Main Battery	• 6-cell (standard), 10.8V, 5200 mAh, 56 Wh • 9-cell (optional), 10.8V, 7800 mAh, 84 Wh • Removable, Lithium ion • Warm-swappable
Bridge Battery	• 6-cell NiMH, 35 mAh • Life (with Suspend-to-RAM on bridge battery only): 5 minutes from full charge
AC Adapter	• Autosensing 100 - 240V, supplying 16 VDC, with a current of 3.75 A
Environmental Specifications	
Temperature	Operating: 41° - 95° F (5° - 35° C) Non-operational: 5° - 140° F (-15° - 60° C)

Stylistic ST5000 Specifications (Continued)	
Humidity	Operating: 20 - 85% non-condensing Non-operating: 8 - 85% non-condensing
Agency Approval Specifications	
Emissions	• EN55022 (CISPR22) Class B • FCC 15/15E, Class B • VCCI Class B
Immunity	• EN55024 (1998)
Safety	• UL and cUL Listed, UL 60950, 3rd edition • CB Report, IEC 60950, 3rd Edition
Specific Absorption Rate (SAR)	• FCC/RSS • ACA/EN
Wireless	• EN300328 • EN301489 • EN301893 • FCC 15E • RSS210 • RSS220
Telecom	• FCC Part 68 • IC CS-03
Other	• Energy Star
Additional Specifications	
Security Features	• Security Panel • Fingerprint Swipe Sensor (12.1" model only) • Trusted Platform Module (TPM)
Operating Systems	• Microsoft® Windows® XP Tablet PC Edition 2005

* Optional feature

Regulatory Information

NOTICE

Changes or modifications not expressly approved by Fujitsu could void this user's authority to operate the equipment.

FCC NOTICES

Notice to Users of Radios and Television

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules.

These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet that is on a different circuit than the receiver.
- Consult the dealer or an experienced radio/TV technician for help.

Shielded interconnect cables must be employed with this equipment to ensure compliance with the pertinent RF emission limits governing this device.

Notice to Users of the US Telephone Network

This equipment (FMD MBH7MD33 Modem) complies with Part 68 of the FCC rules, and the requirements adopted by ACTA. On the bottom of this equipment is a label that contains, among other information, the FCC registration number and ringer equivalence number (REN) for this equipment; or a product identifier in the format US:AAAEQ##TXXXX. If requested, this information or number must be provided to the telephone company.

This equipment is designed to be connected to the telephone network or premises wiring using a standard jack type USOC RJ11C. A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant.

The ringer equivalent number (REN) of this equipment is 0.1B as shown on the label. The REN is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone may result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company.

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could effect the operation of the equipment. If this happens the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please refer to the manual or contact Fujitsu Computer Systems Corporation, Customer Service. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

The equipment cannot be used on public coin service provided by the telephone company. Connection to party line service is subject to state tariffs. (Contact the state public utility commission, public service commission or corporation commission for information).

If your home has specially wired alarm equipment connected to the telephone line, ensure the installation of this computer does not disable your alarm equipment. If you have any questions about what will disable alarm equipment, consult your telephone company or a qualified installer.

The Telephone Consumer Protection Act of 1991 makes it unlawful for any person to use a computer or other electronic device to send any message via a telephone fax machine unless such message clearly contains in a margin at the top or bottom of each transmitted page or on the first page of the transmission, the date an time it is sent and an identification of the business or other entity, or other individual sending the message and the telephone number of the sending machine or such business, other entity, or individual.

DOC (INDUSTRY CANADA) NOTICES

Notice to Users of Radios and Television

This Class B digital apparatus meets all requirements of Canadian Interference-Causing Equipment Regulations.

CET appareil numérique de la class B respecte toutes les exigence du Réglement sur le matérial brouilleur du Canada.

Notice to Users of the Canadian Telephone Network

NOTICE: This equipment (Modem FMD MBH7MD33) meets the applicable Industry Canada Terminal Equipment Technical Specifications. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specifications were met. It does not imply that Industry Canada approved the equipment.

Before connecting this equipment to a telephone line the user should ensure that it is permissible to connect this equipment to the local telecommunication facilities. The user should be aware that compliance with the certification standards does not prevent service degradation in some situations.

Repairs to telecommunication equipment should be made by a Canadian authorized maintenance facility. Any repairs or alterations not expressly approved by Fujitsu or any equipment failures may give the telecommunication company cause to request the user to disconnect the equipment from the telephone line.

NOTICE: The Ringer Equivalence Number (REN) for this terminal equipment is 0.1. The REN assigned to each terminal equipment provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed five.

For safety, users should ensure that the electrical ground of the power utility, the telephone lines and the metallic water pipes are connected together. Users should NOT attempt to make such connections themselves but should contact the appropriate electric inspection authority or electrician. This may be particularly important in rural areas.

Avis Aux Utilisateurs Du Réseau Téléphonique Canadien

AVIS: Le présent matériel (FMD MBH7MD33 Modem) est conforme aux spécifications techniques d'Industrie Canada applicables au matériel terminal. Cette conformité est confirmée par le numéro d'enregistrement. Le sigle IC, placé devant le numéro d'enregistrement, signifie que l'enregistrement s'est effectué conformément à une déclaration de conformité et indique que les spécifications techniques d'Industrie Canada ont été respectées. Il n'implique pas qu'Industrie Canada a approuvé le matériel.

Avant de connecter cet équipement à une ligne téléphonique, l'utilisateur doit vérifier s'il est permis de connecter cet équipement aux installations de télécommunications locales. L'utilisateur est averti que même la conformité aux normes de certification ne peut dans certains cas empêcher la dégradation du service.

Les réparations de l'équipement de télécommunications doivent être eVectuées par un service de maintenance agréé au Canada. Toute réparation ou modification, qui n'est pas expressément approuvée par Fujitsu, ou toute défaillance de l'équipement peut entraîner la compagnie de télécommunications à exiger que l'utilisateur déconnecte l'équipement de la ligne téléphonique.

AVIS: L'indice d'équivalence de la sonnerie (IES) du présent matériel est de 0.1. L'IES assigné à chaque dispositif terminal indique le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas 5.

Pour assurer la sécurité, les utilisateurs doivent vérifier que la prise de terre du service d'électricité, les lignes télphoniques et les conduites d'eau métalliques sont connectées ensemble. Les utilisateurs NE doivent PAS tenter d'établir ces connexions eux-mêmes, mais doivent contacter les services d'inspection d'installations électriques appropriés ou un électricien. Ceci peut être particulièrement important en régions rurales.

Appendix A

Wireless LAN/Bluetooth*
User's Guide

* Optional devices

FCC REGULATORY INFORMATION

Please note the following regulatory information related to the optional wireless LAN module.

Regulatory Notes and Statements

Wireless LAN, Health and Authorization for use

Radio frequency electromagnetic energy is emitted from Wireless LAN devices. The energy levels of these emissions, however, are far much less than the electromagnetic energy emissions from wireless devices such as mobile phones. Wireless LAN devices are safe for use by consumers because they operate within the guidelines found in radio frequency safety standards and recommendations. The use of Wireless LAN devices may be restricted in some situations or environments, such as:

- On board an airplane, or
- In an explosive environment, or
- In situations where the interference risk to other devices or services is perceived or identified as harmful.

In cases in which the policy regarding use of Wireless LAN devices in specific environments is not clear (e.g., airports, hospitals, chemical/oil/gas industrial plants, private buildings), obtain authorization to use these devices prior to operating the equipment.

Regulatory Information/Disclaimers

Installation and use of this Wireless LAN device must be in strict accordance with the instructions included in the user documentation provided with the product. Any changes or modifications made to this device that are not expressly approved by the manufacturer may void the user's authority to operate the equipment. The manufacturer is not responsible for any radio or television interference caused by unauthorized modification of this device, or the substitution or attachment of connecting cables and equipment other than those specified by the manufacturer. It is the responsibility of the user to correct any interference caused by such unauthorized modification, substitution or attachment. The manufacturer and its authorized resellers or distributors will assume no liability for any damage or violation of government regulations arising from failure to comply with these guidelines.

This device must not be co-located or operating in conjunction with any other antenna or transmitter.

For Atheros Wireless LAN:
For operation within 5.15~5.25GHz frequency range, it is restricted to indoor environment, and the antenna of this device must be integral.

Federal Communications Commission statement

This device complies with Part 15 of FCC Rules.

Operation is subject to the following two conditions: (1) This device may not cause interference, and, (2) This device must accept any interference, including interference that may cause undesired operation of this device.

FCC Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. If not installed and used in accordance with the instructions, it may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the distance between the equipment and the receiver.
3. Connect the equipment to an outlet on a circuit different from the one the receiver is connected to.
4. Consult the dealer or an experienced radio/TV technician for help.

FCC Radio Frequency Exposure statement

The available scientific evidence does not show that any health problems are associated with using low power wireless devices. There is no proof, however, that these low power wireless devices are absolutely safe. Low power wireless devices emit low levels of radio frequency energy (RF) in the microwave range while being used. Whereas high levels of RF can produce health effects (by heating tissue), exposure to low-level RF that does not produce heating effects causes no known adverse health effects. Many studies of low-level RF exposure have not found any biological effects. Some studies have suggested that some biological effects might occur, but such findings have not been confirmed by additional research. The wireless LAN radio device has been tested and found to comply with FCC radiation exposure limits set forth for an uncontrolled equipment and meets the FCC radio frequency (RF) Exposure Guidelines in Supplement C to OET65.

The maximum SAR values measured from the devices are:

- Intel PROSet Wireless LAN: 0.921 W/kg
- Atheros Wireless LAN: 1.53 W/kg
- Intel PROSet Wireless LAN + Bluetooth Simultaneous: 0.500 W/kg
- Atheros Wireless LAN + Bluetooth Simultaneous: 1.04 W/kg

Export restrictions

This product or software contains encryption code which may not be exported or transferred from the US or Canada without an approved US Department of Commerce export license. This device complies with Part 15 of FCC Rules., as well as ICES 003 B / NMB 003 B. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesirable operation. Modifications not expressly authorized by Fujitsu Computer Systems Corporation may invalidate the user's right to operate this equipment.

Canadian Notice

To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors is subject to licensing.

High-power radars are allocated as the primary users of 5250 - 5350 MHz and 5650 - 5850 MHz, and these radars could cause interference and/or damage to LELAN (license exempt LAN) devices operating in these bands.

Before Using the Wireless LAN

The Integrated Wireless LAN is a standard device on Stylistic ST5000 Tablet PC's, and an option on Stylistic ST5000D Tablet PC's. This manual describes the basic operating procedures for the wireless LAN (referred to as the "wireless module" in this manual) and how to set up a wireless LAN network. Before using the wireless module, read this manual carefully to ensure correct operation of the device. Keep this manual in a safe place for reference while using the wireless module.

Types of Wireless LANs Covered by this Document

This document is applicable to systems containing one of the following two wireless modules. Most of the procedures are identical. Sections that differ between the two devices have been noted in the text:

- Intel PROSet Wireless LAN (WM3B2915ABG)
- Atheros Wireless LAN (WLL4070)

If your system is a Stylistic ST5000 model, your wireless module is the Intel PROSet wireless LAN; if your system is a Stylistic ST5000D model, your wireless module is the Atheros wireless LAN.

Characteristics of the Wireless Module

This wireless module is a mini-PCI card attached to a mini-PCI slot inside the computer.

The main characteristics are as follows:

- It operates in the 2.4 GHz Industrial, Scientific, and Medical (ISM) RF band; additionally, the Atheros wireless LAN operates in both the 2.4 GHz and 5 GHz RF bands.
- It does not require an FCC license to operate.
- It uses Direct Sequence Spread Spectrum (DSSS), an RF modulation scheme that is resistant to noise.
- This wireless module is Wi-Fi compliant. The wireless module can communicate at a maximum data rate of 54 Mbps.
- The maximum communication range is approximately 80 feet (25 meters) inside a building. Please note that the range you achieve may be shorter or longer than 80 feet, depending on factors such as obstructions, walls, columns, construction material, and reflective objects.
- The wireless modules support a number of industry-standard security mechanisms, including WEP, WPA, TKIP, and 802.1x/EAP (LEAP, TLS, PEAP, MD5).

Wireless LAN Modes Using this Wireless Module

Ad Hoc Mode *(See Figure A-1)*

"Ad Hoc Mode" refers to a type of wireless network that involves connecting multiple computers without the use of an Access Point. Network connectivity between computers can be established using only wireless LAN cards in a peer-to-peer fashion.

Ad Hoc networks are an easy and inexpensive method for establishing network connectivity between multiple computers.

In Ad Hoc mode, you can use Microsoft Network functions, such as File and Print Sharing to share folders, printers, or other peripheral devices, and exchange files with other computers.

To use Ad Hoc Mode, you must set the same SSID and the same encryption key for all the computers that are connected. Communication between computers in an Ad Hoc network will occur provided they are within each other's RF coverage area.

Figure A-1. Ad Hoc Mode Network

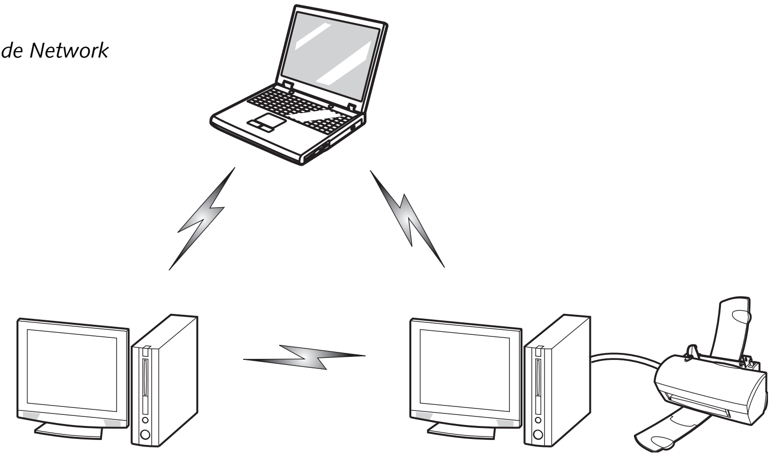
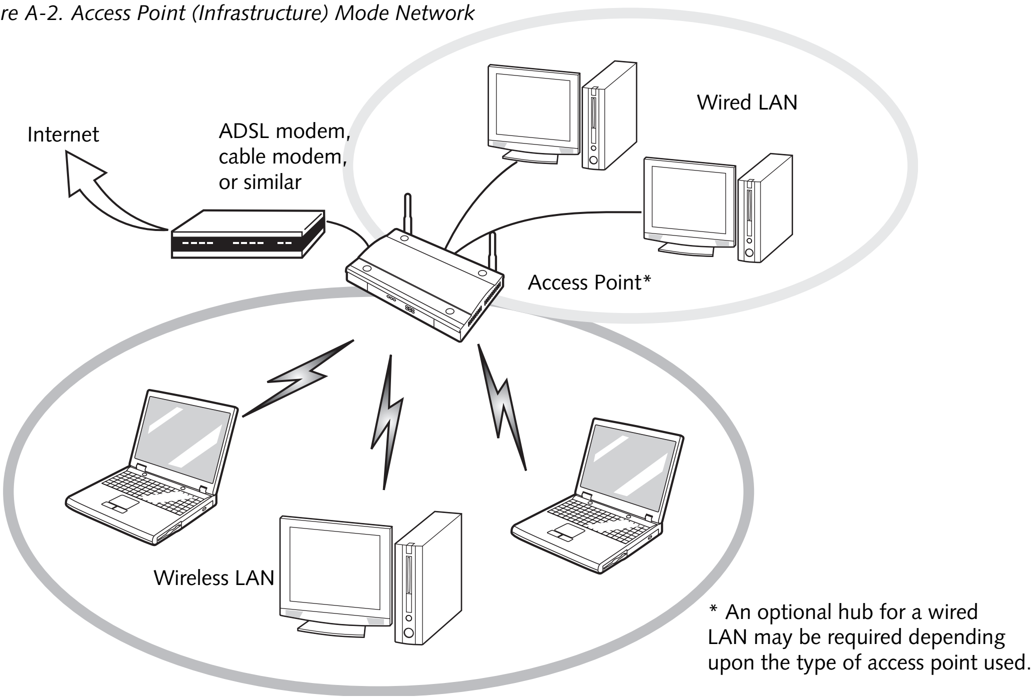


Figure A-2. Access Point (Infrastructure) Mode Network


Internet
ADSL modem, cable modem, or similar
Wired LAN
Access Point*
Wireless LAN
* An optional hub for a wired LAN may be required depending upon the type of access point used.

Access Point (Infrastructure) Mode *(See Figure A-2)*

Infrastructure mode refers to a wireless network in which devices communicate with each other by first going through an Access Point (AP). In infrastructure mode, wireless devices can communicate with each other or can communicate with a wired network. Most corporate wireless LANs operate in infrastructure mode because they require access to the wired LAN in order to use services such as file servers or printers.

How to Handle This Wireless Module

The Integrated Wireless LAN device is already installed in your mobile computer. Under normal circumstances, it should not be necessary for you to remove or re-install it. The wireless LAN has been configured to support the operating system with which your system shipped.

FOR BETTER COMMUNICATIONS

This personal computer may not operate properly due to the operating environment. It is highly recommended that you observe the following precautions when using your wireless LAN module:

- For optimum wireless communications, it recommended that operation of the wireless LAN module occur within 25 meters of the Access Point. Wireless range is dependent on a multitude of factors including number of obstructions, walls, type of construction material, reflective objects, etc.
- If the computer is unable to communicate properly, change the channel to be used or the installation location. During the use of a microwave oven or other equipment generating strong high-frequency energy, in particular, the personal computer may be highly susceptible to the energy and unable to communicate properly.
- Broadcast stations or wireless communication equipment that operate in the 2.4GHz or 5GHz RF Frequency band may interfere with the operation of the wireless LAN module. Increasing of transmit power or relocating Access Points may be necessary to combat the effects of the interference.

STOPPING TRANSMISSION

To use this product inside hospitals, clinics, or airplanes, or in other places where the use of electronic equipment is regulated, stop the transmission of radio waves from the wireless LAN beforehand.

Deactivation using the wireless switch

The transmission of radio waves from the wireless LAN can be stopped by setting the wireless switch to the Off position. Note that the wireless LAN On/Off switch has no effect on non-wireless LAN models.

(See Figure 3 for Wireless LAN switch location.)

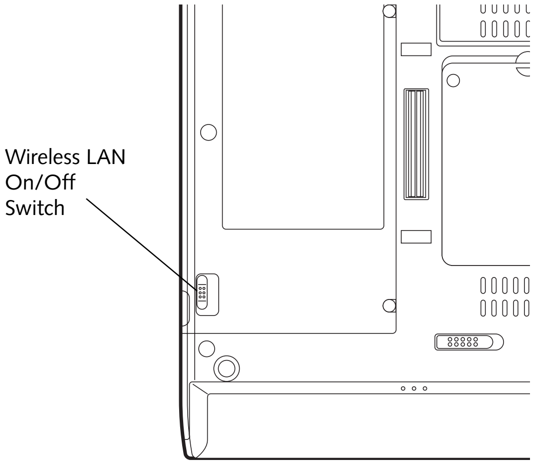


Figure A-3. Wireless LAN On/Off Switch

Deactivation using Windows

Intel PROSet Wireless LAN:

1. Click [Start] --> [(All) Programs] --> [Intel Network Adapters] --> [Intel(R) PROSet]. The Intel(R) PROSet window will be displayed.
2. Click the General tab.
3. Select [Off] for the wireless communications Switch Radio: function, and then click the [OK] button. Wireless communications on/off switching will be deactivated and the transmission of radio waves from the wireless LAN will be stopped.

> To restart transmission, select [On] for the wireless communications Switch Radio: function, and then click the [OK] button.

Atheros Wireless LAN

1. Click [Start] --> [Control Panel] --> [Atheros Client Utility]. The Atheros Wireless Configuration Utility window will be displayed.
2. Click the Wireless Networks tab.
3. Click the [Enable Radio] box to clear it, then click the [OK] button. Wireless communications on/off switching will be deactivated and the transmission of radio waves from the wireless LAN will be stopped.

> To restart transmission, check the [Enable Radio] checkbox to select it., then click the [OK] button.

STARTING TRANSMISSION

To communicate using the wireless LAN function, set the computer to a status from which it can transmit, as follows:

Intel PROSet Wireless LAN:

1. Set the wireless switch to the On position.
2. Click [Start] --> [(All) Programs] --> [Intel Network Adapters] --> [Intel(R) PROSet]. The Intel(R) PROSet window will be displayed.
3. Click the [General] tab if it is not already selected.
4. Select [ON] for the Switch radio: function, then click [OK]. Wireless communications on/off switching will be activated and the transmission of radio waves will be restarted.

Atheros Wireless LAN:

1. Click the Wireless Network Connection icon in the system tray at the lower right of your screen.
2. Click [Enable Radio]. The radio will be turned on.
   Access Point Mode: Transmission is enabled.
   Ad Hoc Mode: Restart your computer to enable the radio.

Connecting the WLAN

FLOW OF OPERATIONS

The wireless LAN connection procedure contained in this section is outlined below.

1. Make sure the mobile computer is ready for the transmission of radio waves from the wireless LAN. For further details, see *(See Starting Transmission on page 50 for more information.)*.
2. Assign the parameters required for wireless LAN connection. *(See Preparation for wireless LAN connection on page 51 for more information.)*.
   - Configure network name (SSID).
   - Configure wireless LAN security parameters as appropriate (e.g., WEP, TKIP, 802.1x/EAP).
3. Perform setting operations relating to network connection. *(See Connection to the network on page 53 for more information.)*

- Specify TCP/IP as the protocol, and confirm the name of the work group and other settings.
- Enter the data required for file/printer sharing on the network. Perform this operation as required.
- For access point (or "infrastructure") connection, configure the wireless module with appropriate parameters required to associate to the access point network.
- Verify that you are able to connect your computer to the network.

PREPARATION FOR WIRELESS LAN CONNECTION

This section explains the preparations required to use the wireless LAN when using the Windows XP Wireless Zero Configuration Tool. Configuration can also be accomplished using the wireless module (Intel or Atheros) configuration utility.

Assigning parameters

Enter the network name (SSID), the network key, and other data required for wireless LAN connection. If there is the administrator of the network, contact the network administrator for data settings.

- To use access point (infrastructure) connection, refer to the access point manual for the access point-setting procedure.
- You do not need to set the channel when using access point (infrastructure) mode. Channel selection is controlled by the access point. In ad hoc networks, channel selection defaults to channel 11; however, channel selection can be manually changed if desired. This can be accomplished only when using the client utility.

  If it is necessary to change the channel, change the setting of the access point. For the setting procedure, refer to the manual of the access point.

1. Make sure the Wireless LAN switch is switched on.
2. Click the [Start] button first and then [Control Panel].
3. If the Control Panel is in Category view, switch to Classic view by clicking "Switch to Classic View" under Control Panel the left frame. (If you are already in Classic view, "Switch to Category View" will be displayed instead.)
4. Double-click the Network Connections icon. A list of currently installed networks will be displayed.
5. Right-click [Wireless Network Connection] in the list, and then click [Properties] in the menu displayed. The [Wireless Network Connection Properties] window will be displayed.
6. Click the [Wireless Networks] tab.
7. Click [Refresh], then choose the correct SSID from the [Available Networks] window. Click [Configure] and proceed to step 10. If the SSID of your access point does not appear in the list, click [Add]. The [Wireless Network Properties] window will be displayed.
8. Select the Association tab if it is not already selected.
9. Enter the information required for connection to the wireless LAN.

   a. Enter the network name (SSID). (i.e., Enter the name of the desired network in less than 33 ASCII characters).

For ad hoc connection: Assign the same network name to all the personal computers to be connected.

For access point (infrastructure) connection: Assign the appropriate SSID. The SSID must be identical to the SSID of the access point. Refer to the access point manual, or contact your network administrator.

b. **For ad hoc connection**, check the following field. **For access point (infrastructure) connection**, clear the check mark for the following field:

[This is a computer-to-computer (ad hoc) network; wireless access points are not used.]

10. Choose the appropriate Network Authentication type. Options are Open, Shared, WPA, or WPA-PSK. Please contact your network administrator for the correct setting.

> It is strongly recommended that you enter the network key for encoding communications data. If the network key is not entered, since the network can be accessed from all personal computers containing the wireless LAN function, there is the danger of your data being stolen or damaged by other users.

11. Choose the Data Encryption type. Options are WEP, TKIP, or AES. The latter two encryption methods are available only when the Network Authentication scheme is WPA or WPA-PSK. WEP, TKIP, and AES are different methods used to encrypt communications data. Proceed to Step 11a if using static WEP keys, otherwise proceed to step 12.

a. Clear the check mark from the [The key is provided for me automatically] check box.

b. Enter data in [Network Key]. Depending on the number of entered characters or digits, whether the key is an ASCII character code or a hexadecimal code will be identified automatically.

- Use five or thirteen characters to enter the key in the **ASCII** character code format. The characters that can be used as the “network key” are as follows: 0 - 9, A - Z, _ (underscore), or,
- Use 10 or 26 characters to enter the key in the **hexadecimal** character code format. The characters that can be used as the “network key” in this case are as follows: 0- 9, A - Z, a - f
  For ad hoc connection: Assign the same network key to all the personal computers to be connected.
  For access point (infrastructure) connection: Assign the identical network key that is programmed into the access point. For this setting, refer to the access point manual or contact your network administrator.

c. Confirm the Network key by re-entering the same data in the [Confirm network key:] field.

d. Make sure that the key index used is identical to the key index used by the Access Point(s).

12. Click the [Authentication] tab and then verify the settings of [Enable network access control using IEEE 802.1x].

For internal use at an organization such as a company, when access by wireless LAN clients is to be limited using IEEE 802.1x authentication, check the [Enable network access control using IEEE 802.1x] check box.

For home use, clear the check mark from [Enable network access control using IEEE 802.1x].

For the setting method relating to IEEE 802.1x authentication, refer to the manual of the access point which you are using.

13. After completion of setting operations, click the [OK] button. Processing will return to the [Wireless Network Connection Properties] window.

14. Verify that the network name entered in step 7 above is added in [Preferred Networks], and then click the [OK] button.

> In [Preferred Networks], register only the desired connection settings.

15. Close the [Wireless Network] window.

CONNECTION TO THE NETWORK

This section explains connection to the network.

If there is an administrator of the network, contact the network administrator for data settings.

Setting the network

Perform the "Setting TCP/IP" and "Confirming the computer and work group names" operations required for network connection.

Setting TCP/IP

To change the setting of the IP address, you need to be logged in from Windows as an administrator.

1. Click the [Start] button first and then [Control Panel].
2. If the Control Panel is in Category view, switch to Classic view by clicking "Switch to Classic View" under Control Panel the left frame. (If you are already in Classic view, "Switch to Category View" will be displayed.)
3. Double-click [Network Connections]. A list of currently installed networks will be displayed.
4. Right-click [Wireless Network Connection] in the list, and then click [Properties] in the menu displayed. The [Wireless Network Connection Properties] window will be displayed.
5. Click the [General] tab if it is not already selected.
6. Click [Internet Protocol (TCP/IP] and then click [Properties]. The [Internet Protocol (TCP/IP) Properties] window will be displayed.
7. Set the IP address as follows:
   - **For ad hoc connection**: Select [Use the following IP address:] and then enter data for [IP address] and [Subnet mask]. See page 62 for IP address setting.
   - **For access point (infrastructure) connection:** If your network uses DHCP, select [Obtain an IP address automatically] and [Obtain DNS server address automatically]. If your network uses static IP addresses, consult with your network administrator for the correct IP address settings.
8. Click the [OK] button. Processing will return to the [Wireless Network Connection Properties] window.
9. Click the [OK] button.
10. Close the [Network Connection] window.

Following this operation, confirm the names of the computer and the workgroup as follows.

Confirming the computer and work group names

To modify the computer name and/or the work group name, you need to be logged in from Windows as an administrator.

1. Click the [Start] button, then [Control Panel].
2. If the Control Panel is in Category view, switch to Classic view by clicking "Switch to Classic View" under Control Panel the left frame. (If you are already in Classic view, "Switch to Category View" will be displayed.)
3. Double-click the [System] icon. The [System Properties] window will be displayed.
4. Click the [Computer Name] tab.
5. Confirm the settings of [Full computer name:] and [Workgroup:].

   a. The setting of [Full computer name:] denotes the name for identifying the computer. Any name can be assigned for each personal computer.

   To change the name, click [Change] and then proceed in accordance with the instruction messages displayed on the screen.

   Enter the desired name in less than 15 ASCII character code format. Identifiability can be enhanced by entering the model number, the user name, and other factors.

   b. [Workgroup name] is the group name of the network. Enter the desired name in less than 15 ASCII character code format.

   For ad hoc connection: Assign the same network name to all personal computers existing on the network.

   For access point (infrastructure) connection: Assign the name of the work group to be accessed.

6. Click the [OK] button. If a message is displayed that requests you to restart the personal computer, click [Yes] to restart the computer.

Setting the sharing function

Set the sharing function to make file and/or printer sharing with other network-connected personal computers valid.

This operation is not required unless the sharing function is to be used.

The folder and printer for which the sharing function has been set will be usable from any personal computer present on the network.

To share a file and/or the connected printer, you need to be logged in as an administrator.

Setting the Microsoft network-sharing service

1. Click the [Start] button first and then [Control Panel].
2. If the Control Panel is in Category view, switch to Classic view by clicking "Switch to Classic View" under Control Panel the left frame. (If you are already in Classic view, "Switch to Category View" will be displayed.)
3. Double-click [Network Connections]. A list of currently installed networks will be displayed.
4. Right-click [Wireless Network Connection] in the list, and then click [Properties] in the menu displayed. The [Wireless Network Connection Properties] window will be displayed.
5. **If [File and Printer Sharing for Microsoft Networks] is displayed, proceed to step 6.** If [File and Printer Sharing for Microsoft Networks] is not displayed, skip to step 7.
6. Make sure that the [File and Printer Sharing for Microsoft Networks] check box is checked, and then click the [OK] button. Skip to "Setting file-sharing function".
7. Click [Install]. The [Select Network Component Type] window will be displayed.
8. Click [Service], then click the [Add] button. The [Select Network Service] window will be displayed.
9. Click [File and Printer Sharing for Microsoft Networks] and then click the [OK] button. Processing will return to the [Wireless Network Connection Properties] window, and [File and Printer Sharing for Microsoft Networks] will be added to the list.
10. Click the [Close] button.

Setting the file-sharing function

The procedure for setting the file-sharing function follows, with the "work" folder in drive C: as an example.

1. Click the [Start] button first and then [My Computer].
2. Double-click [Local disk (C:)].
3. Right-click the "work" folder (or whichever folder you want to share), and then click [Sharing and Security...] in the menu displayed. The [*Folder Name* Properties] window will be displayed.

Setting the file-sharing function for the file which has been used to execute Network Setup Wizard is suggested on the screen. For the wireless LAN, however, since security is guaranteed by entry of the network name (SSID) and the network key, the steps to be taken to set the file-sharing function easily without using Network Setup Wizard are given below.

4. Click [Sharing] if it isn't already selected.
5. Click the link stating "If you understand the security risks, but want to share files without running the wizard, click here".
6. Click "Just enable file sharing" and click [OK].
7. Check the [Share this folder on the network] check box.

To specify the corresponding folder as a read-only folder, select the [Read only] checkbox under the General tab.

8. Click the [OK] button. The folder will be set as a sharable folder, and the display of the icon for the "work." folder will change.

Setting the printer-sharing function

1. Click the [Start] button first and then [Printers and FAX]. A list of connected printers will be displayed.
2. Right-click the printer for which the sharing function is to be set, and then click [Sharing] in the menu displayed. The property window corresponding to the selected printer will be displayed.

Setting the printer-sharing function when Network Setup Wizard has been executed is suggested on the screen. For the wireless LAN, however, since security is guaranteed by entry of the network name (SSID) and the network key, the steps to be taken to set the printer-sharing function without using Network Setup Wizard are laid down below.

3. Click the [Sharing] tab.
4. Click [Share this printer].

5. Enter the sharing printer name in [Share name].

6. Click the [OK] button.

Confirming connection

After you have finished the network setup operations, access the folder whose sharing has been set for other personal computers. Also, confirm the status of the radio waves in case of trouble such as a network connection failure.

> In the case of access point (infrastructure) connection, enter the necessary data for the access point before confirming connection. Refer to the manual of the access point for the access point setup procedure.

Connecting your personal computer to another personal computer

1. Click [Start] first and then [My Computer]. The [My Computer] window will be displayed in the left frame.

2. Click [My Network Places] in the "Other Places" list. The window [My Network Places] will be displayed.

3. Click [View workgroup computers] under Network Tasks in the left frame.

4. Double-click the personal computer to which your personal computer is to be connected. The folder that was specified in "Setting the file-sharing function" on page 54 will be displayed.

5. Double-click the folder to be accessed.

Confirming the status of the radio

Intel PROSet Wireless LAN:

1. Click [Start] -> [All Programs] -> [Intel Network Adapters] -> [Intel(R) PROSet]. The [Intel(R) PROSet] window will be displayed.

2. Click the [General] tab and confirm radio status in the window displayed. The current connection status will be displayed.

   - **Signal Quality**
     The quality of the signals is displayed on a graph.

   - **Network name (SSID)**
     The connected network name (SSID) is displayed.

   - **Profile name**
     "<No profile>" is displayed.

   - **Mode**
     If access point (infrastructure) connection is in use, "Infrastructure (AP)" will be displayed. If ad hoc connection is in use, "Ad hoc (Peer-to-peer)" will be displayed.

   - **Security**
     Displays the encryption type currently used by the radio.

   - **Speed**
     Displays the current data rate used by the radio to transmit and receive data.

   - **Band (Frequency)**
     The current operating frequency band is displayed. When communication is possible, "802.11b (2.4 GHz)" is displayed.

   - **Channel**
     The channel number currently being used for the communications is displayed.

If connection cannot be made to the network or if you want to check for normal connection, see "Troubleshooting" on page 58.

Atheros Wireless LAN:

1. Right-click the Atheros icon in the lower right corner of the screen.

2. Click [Open Client Utility]. The Atheros Wireless Configuration Utility window opens.

3. Contained within the Current Status tab and Advanced Current Status, you will find the current operating status of the radio. (When the radio is turned off or the computer is not yet connected, some of the conditions will not be displayed.)

   - **Profile Name**
     The current configuration profile is displayed.

   - **Network Type - Configured Network Type**
     [Access Point] or [AdHoc] will be displayed.

   - **Current Mode**
     Indicates the frequency and data rate currently used by the radio.

   - **Current Channel**
     The channel number currently used by the radio.

   - **Link Status**
     Displays the current connected state of the WLAN module.

   - **Encryption Type**
     Displays the encryption type currently used by the radio.

- **IP Address**
  Displays the current TCP/IP address assigned to the WLAN adapter.
- **Country**
  The country with the country code for which the radio is configured.
- **Transmit Power Level**
  Displays the current transmit power level of the radio.
- **Network Name (SSID)**
  Displays the Network Name (SSID) currently used by the radio.
- **Power Save Mode**
  Displays the configured Power Save Mode currently used by the radio. [Off], [Normal], or [Maximum] will be displayed.
- **BSSID**
  Displays the Basic Service Set Identifier. This is typically the MAC address of the Access Point or in the case of AdHoc networks, is a randomly generated MAC address.
- **Frequency**
  Displays the center frequency currently being used by the radio.
- **Transmit Rate**
  Displays the current data rate used by the radio to transmit data.
- **Receive Rate**
  Displays the current data rate used by the radio to receive data.

Other settings

SETTING OF POWER-SAVING FUNCTION

You can set the power-saving function of wireless LAN. Default setting is auto-setting. In case of using the power-saving function, manually control the communication performance.

Intel PROSet Wireless LAN:

1. Click [Start] -> [(All) Programs] -> [Intel Network Adapters] -> [Intel(R) PROSet]. The Intel(R) PROSet window will be displayed.
2. Click the [Adapter] tab.
3. Click the [Configure] button in [Power settings]. The [Power settings] window will be displayed.
4. Select [Manual], and adjust the bar to set the power-saving function.

Setting of transmission power during ad hoc connection

By controlling the transmission power during ad hoc connection, you can broaden or narrow the communication range. This setting is only effective during ad hoc connection. It will be ineffective during access point connection.

Intel PROSet Wireless LAN:

1. Click [Start] -> [(All) Programs] -> [Intel Network Adapters] -> [Intel(R) PROSet]. The Intel(R) PROSet window will be displayed.
2. Click the [Adapter] tab.
3. Click the [Configure] button in [Power settings]. The [Power settings] window will be displayed.
4. Adjust the "Transmission Power (Ad Hoc)" bar to set the transmission power.

Setting of channels during ad hoc connection

You can set channels during ad hoc connection. Channel 11 is set by default. When connecting to an existing ad hoc network, no channel setting will be effective.

This setting is only effective during ad hoc connection; it will be ineffective during access point connection.

When changing channels during ad hoc connection, change the channel settings of all connected computers with the same Network name (SSID) at the same time. After changing the channels, turn off all computers and -- after they are all turned off -- turn them back on.

Intel PROSet Wireless LAN:

1. Click [Start] -> [(All) Programs] -> [Intel Network Adapters] -> [Intel(R) PROSet]. The Intel(R) PROSet window will be displayed.
2. Click the [Adapter] tab.
3. Click the [Configure] button in [Ad hoc settings]. The [Ad hoc settings] window will be displayed.
4. Change channels during ad hoc connection by selecting a new channel from the drop down list.
5. Click [OK].

Atheros Wireless LAN:

1. Click on the My Computer icon. Select [View system information] from the left frame.
2. Select the Hardware tab and click [Device Manager].
3. Double-click "Atheros Wireless LAN Adapter" under [Network Adapters].
4. In the Atheros Wireless LAN Adapter window, select the Advanced tab.
5. Select IBSS Channel Number from the list, and change the value from the [Value:] dropdown list to the desired channel.
6. Click [OK].

Troubleshooting

Causes and countermeasures for troubles you may encounter while using your wireless LAN are described in the following table.

Problem	Possible Cause	Possible Solution
Unavailable network connection	**Incorrect network name (SSID) or network key**	**Ad hoc connection:** verify that the network names (SSID's) and network keys (WEP) of all computers to be connected have been configured correctly. SSID's and WEP key values must be identical on each machine. **Access Point (Infrastructure) connection:** set the network name (SSID) and network key to the same values as those of the access point. Set the Network Authentication value identically to that of the Access Point. Please consult your network administrator for this value, if necessary. For the method of setting network authentication, refer to the following pages:· "Assigning parameters" on page 51·
	Poor radio wave condition	Ad hoc connection: Retry connection after shortening the distance to the destination computer or removing any obstacles for better sight. Access Point (Infrastructure) connection: Retry connection after shortening the distance to the access point or removing any obstacles for better sight. To check the wave condition, refer to the following pages:· "Confirming the status of the radio waves" on page 55.·
	Radio wave transmission has stopped	Check if the wireless switch is turned ON. Also verify "Disable Radio" is not checked in "Network setting" window. Refer to "Starting Transmission" on page 50.
	The computer to be connected is turned off	Check if the computer to be connected is turned ON.
	Active channel duplication due to multiple wireless LAN networks	If there is any other wireless LAN network nearby, change channels to avoid active channel duplication. For the method of checking active channels, refer to the following pages:· "Confirming the status of the radio waves" on page 55·
	No right of access to the network to be connected	Check if you have a right of access to the network to be connected with.
	Incorrectly-performed network setting	Check the protocol, work group name or shared setting. For the method of checking, refer to the following pages:· "Connection to the Network" on page 53.
	Unmatched [Network authentication (shared mode)] settings in Windows XP	If the setting of [Network authentication (shared mode)] is not matched with that of access point or computer to be connected with, no communication can be established. Check the parameter setting. Refer to "Assigning parameters" on page 51.

Problem	Possible Cause	Possible Solution
Unavailable network connection **(continued)**	**It takes too long to retrieve the network and display the connected computers.**	Retrieve computers as follow: 1. Click [Start] button, then click [Search]. 2. Click [Computers or people]. 3. Click [Computers on the network]. 4. Input the name of computer to be connected with in [Computer name] and click [Search]. 5. Double-click the icon of connected computer.·
	Incorrect setting of IP address	Check the network setting. "Setting the network" on page 53. In case of using TCP/IP protocol, you can check IP address as follows: 1. Click [Start] -> [All programs] -> [Accessories] -> [Command prompt].· 2. In [Command prompt] or [MS-DOS prompt] window, input [IPCONFIG] command as follows, then press [Enter] key. Example: In case of C drive being the hard disk: C:\ipconfig [Enter] Check that the IP address is correctly displayed:. IP Address................: 10.0.1.3 Subnet Mask.............: 255.255.255.0 Default Gateway.........: 10.0.1.1 When IP address is displayed as [169.254.XXX.YYY] or [0.0.0.0], IP address is not correctly fetched from the access point. In that case, restart the computer itself. If the display is still unchanged, check the setting of TCP/IP. If [Cable Disconnected] or [Media Disconnected] is displayed without showing IP address, check the setting of network name (SSID) and network key. Also, set the network authentication according to the access point.
Communication is disconnected soon after connection to the access point	**Access control may be disabled**	Check the setting of "Enable network access control using IEEE 802.1X".Refer to "Assigning parameters" on page 51. When restricting the access of wireless LAN clients using IEEE802.1X authentication, put a check mark on "Enable network access control using IEEE 802.1X". When using at home, remove a check mark on "Enable network access control using IEEE802.1X". For the method of setting related with IEEE802.1X authentication, refer to the access point manual.
	Authentication method may have been entered incorrectly	Re-enter your WEP key and verify that your authentication method (Open or Shared) is correct.

Wireless LAN Glossary

Access point

A designation of wireless LAN network configurations. It indicates a form of communication using an Access Point. For details, refer to "access point connection" on page 48.

Ad hoc

A designation for wireless LAN network configuration. It indicates a form of communication limited to those personal computers which have wireless LAN function. For details, refer to "Ad hoc connection" on page 48.

Channel

The frequency band of wireless LAN to be used in communications over wireless LAN or at the access point.

DHCP (Dynamic Host Configuration Protocol)

A protocol used for automatically fetching communication parameters such as IP addresses. The side which assigns IP address is called DHCP server and the side that is assigned it is called DHCP client.

DNS (Domain Name System)

A function that controls the correspondence of IP addresses assigned to a computer with the name. Even for those computers whose IP addresses are unknown, if their names are known, it is possible to communicate with them.

IEEE802.11a

One of the wireless LAN standards prescribed by the 802.11 committee in charge of establishing standards of LAN technology in IEEE (Institute of Electrical and Electronic Engineers). It allows communications at the maximum speed of 54 Mbps by using a 5GHz band which can freely be used without radio communication license.

IEEE802.11b

One of the wireless LAN standards prescribed by the 802.11 committee in charge of establishing standards of LAN technology in IEEE (Institute of Electrical and Electronic Engineers). It allows communications at the maximum speed of 11Mbps by a band of 2.4 GHz (ISM band) which can freely be used without radio communication license.

IP address

An address used by computers for communicating in TCP/IP environment. IP addresses have global and private addresses. A global address is a unique address in the world. A private address is a unique address within a closed network.

LAN (Local Area Network)

An environment connecting computers within a relatively small range, such as the same floor and building.

MAC address (Media Access Control Address)

A physical address inherent to a network card. For Ethernet, the top three bytes are controlled/assigned as a vendor code. The remaining three bytes comprise the code uniquely (to avoid duplication) controlled by each vendor. As a result, there is no Ethernet card with the same physical address in the world. In Ethernet, the frame transmission/reception is performed based on this address.

MTU (Maximum Transmission Unit)

The maximum size of data which can be transmitted at one time in networks including the Internet. In an environment whose maximum size of data is too large to correctly receive data, normal communications can be restored by setting the size of MTU to a smaller value.

Network authentication

The method of authentication performed by wireless LAN clients to connect with the access point. There are two types: open system authentication and shared key authentication. The type of authentication must be set to each client and also coincide with the setting of access point with which to communicate. Network authentication is sometimes called authentication mode.

Network key

Data that is used for encrypting data in data communication. The personal computer uses the same network key both for data encryption and decryption, therefore, it is necessary to set the same network key as the other side of communication.

Network name (SSID: Service Set Identifier)

The network name is a unique identifier attached to the WLAN packet header that acts as a password when the client attempts to connect to a WLAN. The SSID differentiates one WLAN from another so all WLAN devices attempting to connect to a specific WLAN must use the same SSID. SSID's are transmitted in cleartext, thus supplying no security to the WLAN.

Open system authentication

An 802.11 wireless LAN authentication method. Open System does not exchange any key or other information, it is a simple request by the mobile station to be authenticated without verifying identity.

PPPoE (Point to Point Protocol over Ethernet)

A method of allowing the authentication protocol adopted in telephone line connection (PPP) to be used over an Ethernet.

Protocol

A procedure or rule of delivering data among computers. Ordered data communication is allowed by making all conditions required for communication including the method of data transmission/reception and actions upon communication errors into procedures.

Shared key authentication

An 802.11 wireless LAN authentication method. When a client attempts to associate to an access point, the access point will send a challenge to the client. The client encrypts the challenge with the network key and sends it back to the access point. If the access point can decrypt the challenge, then authentication has succeeded.

SSID (Service Set Identifier)

See "Network name"

Subnet mask

TCP-IP network is controlled by being divided into multiple smaller networks (subnets). IP address consists of the subnet address and the address of each computer. Subnet mask defines how many bits of IP address comprise the subnet address. The same value shall be set among computers communicating with each other.

TCP/IP (Transmission Control Protocol/Internet Protocol)

A standard protocol of the Internet.

Wi-Fi

Short for "Wireless Fidelity". A term meant to be used generically when referring to any type of 802.11 network, whether 802.11b, 802.11a, 802.11g, etc.

IP address information

ℹ IP addressing is much more complicated than can be briefly explained in this document. You are advised to consult with your network administrator for additional information.

If IP address is unknown, set IP address as follows:

If you have an access point (DHCP server) on the network, set the IP address as follows:

[Obtain an IP address automatically]

ℹ A DHCP server is a server that automatically assigns IP addresses to computers or other devices in the network. There is no DHCP server for the AdHoc network.

If the IP address is already assigned to the computer in the network, ask the network administrator to check the IP address to be set for the computer.

If no access point is found in the network:

An IP address is expressed with four values in the range between 1 and 255.

Set the each computer as follows: The value in parentheses is a subnet mask.

<Example>

Computer A: 192.168.100.2 (255.255.255.0)

Computer B: 192.168.100.3 (255.255.255.0)

Computer C: 192.168.100.4 (255.255.255.0)

:

:

Computer X: 192.168.100.254 (255.255.255.0)

Specifications

Item	Specification
Type of network	Conforms to IEEE 802.11a/802.11b/g (Wi-Fi based)*
Transfer rate	(Automatic switching) 54 Mbps maximum data rate
Active frequency	802.11b/g: 2400~2473 MHz 802.11a: 4900 ~ 5850 MHz
Number of channels	802.11a: 8 independent channels 802.11b/g: 11 channels, 3 non-overlapping channels
Security	• Encryption Types: WEP, TKIP, AES • WPA 1.0 compliant • Encryption Keylengths Supported: 64 bits, 128 bits, 152 bits (Atheros module using AES encryption only) • 802.1x/EAP • CCX 1.0 compliant
Maximum recommended number of computers to be connected over wireless LAN (during ad hoc connection)	10 units or less ***

* "Wi-Fi based" indicates that the interconnectivity test of the organization which guarantees the interconnectivity of wireless LAN (Wi-Fi Alliance) has been passed.

** Encryption with network key (WEP) is performed using the above number of bits, however, users can set 40 bits/104 bits after subtracting the fixed length of 24 bits.

*** The maximum number of computers that can be supported by an Access Point is highly variable, and can be affected by such factors as application bandwidth utilization, broadcast packet traffic, type of applications used, etc. The number of 10 provided by this document is meant only as a guideline and not a limitation of the technology.

Using the Bluetooth Device

The Integrated Bluetooth module (UGXZ5-102A) is an optional device available for Fujitsu mobile computers.

WHAT IS BLUETOOTH?

Bluetooth technology is designed as a short-range wireless link between mobile devices, such as laptop computers, phones, printers, and cameras. Bluetooth technology is used to create Personal Area Networks (PANs) between devices in short-range of each other.

WHERE TO FIND INFORMATION ABOUT BLUETOOTH

The Bluetooth module contains a robust Help user's guide to assist you in learning about operation of the Bluetooth device.

To access the Help file, click [Start] -> All Programs, and click on Toshiba. Select Bluetooth, then select User's Guide.

For additional information about Bluetooth Technology, visit the Bluetooth Web site at: www.bluetooth.com.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

The transmitters in this device must not be co-located or operated in conjunction with any other antenna or transmitter.

Canadian Notice

To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors is subject to licensing.

Warranty

Users are not authorized to modify this product. Any modifications invalidate the warranty.

This equipment may not be modified, altered, or changed in any way without signed written permission from Fujitsu. Unauthorized modification will void the equipment authorization from the FCC and Industry Canada and the warranty.

Appendix B

Security Device* User's Guide

* Availability varies by model

Fingerprint Sensor Device

INTRODUCING THE FINGERPRINT SENSOR DEVICE

Your system may have a fingerprint sensor device on the side of the display opposite the function buttons. The device is a standard feature on 12.1" models; it is not available on 10.4" models. *(See Figure 1-2 on page 3 for location)*

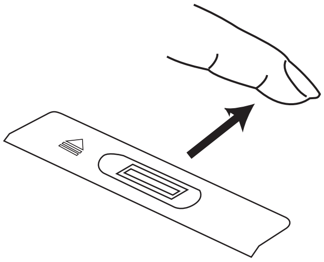


Figure B-1 Fingerprint sensor

With a fingerprint sensor, you can avoid having to enter a username and password every time you want to:

- Log onto Windows
- Recover from suspend mode
- Cancel a password-protected screen saver
- Log into homepages that require a username and password

After you have "enrolled" - or registered - your fingerprint, you can simply swipe your fingertip over the sensor for the system to recognize you.

The fingerprint sensor uses Softex OmniPass which provides password management capabilities to Microsoft Windows operating systems. OmniPass enables you to use a "master password" for all Windows, applications, and on-line passwords.

OmniPass requires users to authenticate themselves using the fingerprint sensor before granting access to the Windows desktop. This device results in a secure authentication system for restricting access to your computer, applications, web sites, and other password-protected resources.

OmniPass presents a convenient graphical user interface, through which you can securely manage passwords, users, and multiple identities for each user.

GETTING STARTED

This section guides you through the preparation of your system for the OmniPass fingerprint recognition application. You will be led through the OmniPass installation process. You will also be led through the procedure of enrolling your first user into OmniPass.

INSTALLING OMNIPASS

If OmniPass has already been installed on your system, skip this section and go directly to "User Enrollment" on page 68. You can determine whether OmniPass has already been installed by checking to see if the following are present:

- The presence of the gold key-shaped OmniPass icon in the system tray at the bottom right of the screen.
- The presence of the Softex program group in the **Programs** group of the **Start** menu

System Requirements

The OmniPass application requires space on your hard drive; it also requires specific Operating Systems (OS's). The minimum requirements are as follows:

- Windows XP Home Edition, Windows XP Professional or Windows 2000 operating system
- At least 35 MB available hard disk space

Installing the OmniPass Application

If OmniPass is already installed on your system, go to "User Enrollment" on page 68. Otherwise continue with this section on software installation.

For installation, OmniPass requires that the user installing OmniPass have administrative privileges to the system. If your current user does not have administrative privileges, log out and then log in as an administrator before proceeding with OmniPass installation.

To install OmniPass on your system you must:

1. Insert the installation media for the OmniPass application into the appropriate drive. If you are installing from CD-ROM or DVD-ROM, you must find and launch the OmniPass installation program (setup.exe) from the media.
2. Follow the directions provided in the OmniPass installation program. Specify a location to which you would like OmniPass installed. It is recommended that you NOT install OmniPass in the root directory (e.g. C:\).
3. Once OmniPass has completed installation you will be prompted to restart you system. Once your system has rebooted you will be able to use OmniPass. If you choose not to restart immediately after installation, OmniPass will not be available for use until the next reboot.

The installation program automatically places an icon (Softex OmniPass) in the Windows Control Panel as well as a golden key shaped icon in the taskbar.

Verifying Information about OmniPass

After you have completed installing OmniPass and restarted your system, you may wish to check the version of OmniPass on your system.

To check the version information of OmniPass:

1. From the Windows Desktop, double-click the key-shaped OmniPass icon in the taskbar (usually located in the lower right corner of the screen),
   or,
   Click the **Start** button, select **Settings**, and click **Control Panel** (if you are using Windows XP you will see the Control Panel directly in the Start menu; click it, then click **Switch to Classic View**). Double-click **Softex OmniPass** in the Control Panel, and the OmniPass Control Center will appear. If it does not appear, then the program is not properly installed,

   or,

   Click the **Start** button, select **Programs**, and from the submenu select the **Softex** program group, from that submenu click **OmniPass Control Center.**
2. Select the **About** tab at the top of the OmniPass Control Panel. The About tab window appears with version information about OmniPass.

Uninstalling OmniPass

For uninstallation, OmniPass requires that the user uninstalling OmniPass have administrative privileges to the system. If your current user does not have administrative privileges, log out and then log in as an administrator before proceeding with OmniPass uninstallation.

To remove the OmniPass application from your system:

1. Click **Start** on the Windows taskbar. Select **Settings**, and then **Control Panel.**
2. Double-click **Add/Remove Programs**.
3. Select **OmniPass**, and then click **Change/Remove**.
4. Follow the directions to uninstall the OmniPass application.
5. Once OmniPass has finished uninstalling, reboot your system when prompted.

USER ENROLLMENT

Before you can use any OmniPass features you must first enroll a user into OmniPass.

Master Password Concept

Computer resources are often protected with passwords. Whether you are logging into your computer, accessing your email, e-banking, paying bills online, or accessing network resources, you often have to supply credentials to gain access. This can result in dozens of sets of credentials that you have to remember.

During OmniPass user enrollment a "master password" is created for the enrolled user. This master password "replaces" all other passwords for sites you register with OmniPass.

Example: A user, John, installs OmniPass on his system (his home computer) and enrolls an OmniPass user with username "John_01" and password "freq14". He then goes to his webmail site to log onto his account. He inputs his webmail credentials as usual (username "John_02" and password "tablet"), but instead of clicking [Submit], he directs OmniPass to **Remember Password.** Now whenever he returns to that site, OmniPass will prompt him to supply access credentials.

John enters his OmniPass user credentials ("John_01" and "freq14") in the OmniPass authentication prompt, and he is allowed into his webmail account. He can do this with as many web sites or password protected resources he likes, and he will gain access to all those sites with his OmniPass user credentials ("John_01" and "freq14"). This is assuming he is accessing those sites with the system onto which he enrolled his OmniPass user. OmniPass does not actually change the credentials of the password protected resource. If John were to go to an Internet cafe to access his webmail, he would need to enter his original webmail credentials ("John_02" and "tablet") to gain access. If he attempts his OmniPass user credentials on a system other than where he enrolled that OmniPass user, he will not gain access.

The basic enrollment procedure assumes you have no hardware authentication devices or alternate storage locations that you wish to integrate with OmniPass. If you desire such functionality, consult the appropriate sections after reviewing this section.

Basic Enrollment

The Enrollment Wizard will guide you through the process of enrolling a user. Unless you specified otherwise, after OmniPass installation the Enrollment Wizard will launch on Windows login. If you do not see the Enrollment Wizard, you can bring it up by clicking **Start** on the Windows taskbar; select **Programs**; select **Softex**; click **OmniPass Enrollment Wizard**.

1. Click **Enroll** to proceed to username and password verification. By default, the OmniPass Enrollment Wizard enters the credentials of the currently logged in Windows user.
2. Enter the password you use to log in to Windows. This will become the "master password" for this

OmniPass user. In most cases, the **Domain:** value will be your Windows computer name. In a corporate environment, or when accessing corporate resources, the **Domain**: may not be your Windows computer name. Click [Next] to continue.

3. In this step OmniPass captures your fingerprint. Refer to "Enrolling a Fingerprint" on page 69 for additional information.
4. Next, choose how OmniPass notifies you of various events. We recommend you keep **Taskbar Tips** on **Beginner mode taskbar tips** and **Audio Tips** on at least **Prompt with system beeps only** until you get accustomed to how OmniPass operates. Click [Next] to proceed with user enrollment. You will then see a Congratulations screen indicating your completion of user enrollment.
5. Click [Done] to exit the OmniPass Enrollment Wizard. You will be asked if you'd like to log in to OmniPass with your newly enrolled user; click [Yes].

Enrolling a Fingerprint

Enrolling a fingerprint will increase the security of your system and streamline the authentication procedure.

You enroll fingerprints in the OmniPass Control Center. With an OmniPass user logged in, double-click the system tray OmniPass icon. Select the **User Settings** tab and click **Enrollment** under the **User Settings** area. Click **Enroll Authentication Device** and authenticate at the authentication prompt to start device enrollment.

1. During initial user enrollment, you will be prompted to select the finger you wish to enroll. Fingers that have already been enrolled will be marked by a green check. The finger you select to enroll at this time will be marked by a red arrow. OmniPass allows you to re-enroll a finger. If you choose a finger that has already been enrolled and continue enrollment, OmniPass will enroll the fingerprint, overwriting the old fingerprint. Select a finger to enroll and click [Next].
2. It is now time for OmniPass to capture your selected fingerprint. It may take a several capture attempts before OmniPass acquires your fingerprint. Should OmniPass fail to acquire your fingerprint, or if the capture screen times out, click [Back] to restart the fingerprint enrollment process.

   Your system has a "swipe" fingerprint sensor. A swipe sensor is small and resembles a skinny elongated rectangle. To capture a fingerprint, gently swipe or pull your fingertip over the sensor (starting at the second knuckle) in the direction of the arrow. Swiping too fast or too slow will result in a failed capture. The **Choose Finger** screen has a [Practice] button; click it to practice capturing your fingerprint. When you are comfortable with how your fingerprint is captured, proceed to enroll a finger.
3. Once OmniPass has successfully acquired the fingerprint, the **Verify Fingerprint** screen will automatically appear. To verify your enrolled fingerprint, place your fingertip on the sensor and hold it there as if you were having a fingerprint captured. Successful fingerprint verification will show a green fingerprint in the capture window and the text **Verification Successful** under the capture window.

USING OMNIPASS

You are now ready to begin using OmniPass. Used regularly, OmniPass will streamline your authentication procedures.

Password Replacement

You will often use the password replacement function. When you go to a restricted access website (e.g., your bank, your web-based email, online auction or payment sites), you are always prompted to enter your login credentials. OmniPass can detect these prompts and you can teach OmniPass your login credentials. The next time you go to that website, you can authenticate with your fingerprint to gain access.

OmniPass Authentication Toolbar

After installing OmniPass and restarting, you will notice a dialog you have not seen before at Windows Logon. This is the OmniPass Authentication Toolbar, and it is displayed whenever the OmniPass authentication system is invoked. The OmniPass authentication system may be invoked frequently: during Windows Logon, during OmniPass Logon, when unlocking your workstation, when resuming from standby or hibernate, when unlocking a password-enabled screensaver, during password replacement for remembered site or application logins, and more. When you see this toolbar, OmniPass is prompting you to authenticate.

The **Logon Authentication** window indicates what OmniPass-restricted function you are attempting. The icons in the lower left (fingerprint and key) show what authentication methods are available to you. Selected authentication methods are highlighted while unselected methods are not. When you click the icon for an unselected authentication method, the authentication prompt associated with that method is displayed.

When prompted to authenticate, you must supply the appropriate credentials: an enrolled finger for the fingerprint capture window or your master password for the master password prompt (the key icon).

Remembering a Password

OmniPass can remember any application, GUI, or password protected resource that has a password prompt.

Using the following procedure, you can store a set of credentials into OmniPass. These credentials will then be linked to your "master password" or fingerprint.

Go to a site that requires a login (username and password), but *do not log in yet.* At the site login prompt, enter your username and password in the prompted fields, but *do not enter the site* (do not hit [Enter], [Submit], [OK], or Login). Right-click the OmniPass system tray icon and select **Remember Password** from the submenu. The Windows arrow cursor will change to a golden key OmniPass cursor. Click this OmniPass cursor in the login prompt area, but do not click the [Login] or [Submit] button.

Associating a Friendly Name
After clicking the OmniPass key cursor near the login prompt, OmniPass will prompt you to enter a "friendly name" for this site. You should enter something that reminds you of the website, the company, or the service you are logging into. In its secure database, OmniPass associates this friendly name with this website.

Additional Settings for Remembering a Site
When OmniPass prompts you to enter a "friendly name" you also have the opportunity to set how OmniPass authenticates you to this site. There are three effective settings for how OmniPass handles a remembered site.

The default setting is **Automatically click the "OK" or "Submit" button for this password protected site once the user is authenticated**. With this setting, each time you navigate to this site OmniPass will prompt you for your master password or fingerprint authentication device. Once you have authenticated with OmniPass, you will automatically be logged into the site.

Less secure is the option to **Automatically enter this password protected site when it is activated. Do not prompt for authentication**. Check the upper box to get this setting, and each time you navigate to this site OmniPass will log you into the site without prompting you to authenticate.

This setting is more convenient in that whenever you go to a site remembered with this setting, you will bypass any authentication procedure and gain instant access to the site. But should you leave your system unattended with your OmniPass user logged in, anyone using your system can browse to your password protected sites and gain automatic access.

If you uncheck both boxes in **Settings for this Password Site,** OmniPass will prompt you for your master password or fingerprint authentication device. Once you have authenticated with OmniPass your credentials will be filled in to the site login prompt, but you will have to click the website [OK], [Submit], or [Login] button to gain access to the site.

Click **Finish** to complete the remember password procedure. The site location, the credentials to access the site, and the OmniPass authentication settings for the site are now stored in the OmniPass secure database. The OmniPass authentication settings (**Settings for this Password Site**) can always be changed in **Vault Management**.

Logging in to a Remembered Site

Whether or not OmniPass prompts you to authenticate when you return to a remembered site is determined by **Settings for this Password Site** and can be changed in **Vault Management**.

The following cases are applicable to using OmniPass to login to: Windows, remembered web sites, and all other password protected resources.

With Master Password
Once you return to a site you have remembered with OmniPass, you may be presented with a master password prompt. Enter your master password and you will be allowed into the site.

Logging into Windows with a Fingerprint Device
When logging into Windows with a fingerprint device, the fingerprint capture window will now appear next to the Windows Login screen. Place your enrolled fingertip on the sensor to authenticate. You will be simultaneously logged into Windows and OmniPass. The capture window will also appear if you have used **Ctrl-Alt-Del** to lock a system, and the fingerprint device can be used to log back in as stated above.

If a machine is locked and OmniPass detects a different user logging back in with a fingerprint, the first user will be logged out and the second user logged in.

In Windows XP, your login options must be set either for classic login, or for fast user switching and logon screen to be enabled to use your fingerprint to log on to Windows. To change this go to **Control Panel**, select **User Accounts** and then click **Change the way users log on or off**. If your Windows screensaver is password protected, the fingerprint capture window will now appear next to screensaver password dialog during resume. You can authenticate to your screensaver password prompt with your enrolled finger.

Password Management

OmniPass provides an interface that lets you manage your passwords. To access this GUI, double-click the

OmniPass key in the system tray. Click **Vault Management**; you will be prompted to authenticate. Once you gain access to **Vault Management**, click **Manage Passwords** under **Vault Settings**. You will see the **Manage Passwords** interface, with a list of friendly names.

You can view the credentials stored for any remembered website by highlighting the desired resource under **Password Protected Dialog** and clicking **Unmask Values**. Should a password be reset, or an account expire, you can remove stored credentials from OmniPass. Highlight the desired resource under **Password Protected Dialog** and click **Delete Page**. You will be prompted to confirm the password deletion.

The two check boxes in **Manage Passwords** govern whether OmniPass prompts you to authenticate or directly logs you into the remembered site.

OmniPass will overwrite an old set of credentials for a website if you attempt to use **Remember Password** on an already remembered site.

The exception to the above rule is the resetting of your Windows password. If your password is reset in Windows, then the next time you login to Windows, OmniPass will detect the password change and prompt you to "Update" or "Reconfirm" your password with OmniPass. Enter your new Windows password in the prompt(s) and click **OK** and your OmniPass "master password" will still be your Windows password.

OmniPass User Identities

Identities allow OmniPass users to have multiple accounts to the same site (e.g., *bob@biblomail.com* and *boballen@biblomail.com*). If OmniPass did not provide you identities, you would be limited to remembering one account per site.

To create and manage identities, double-click the OmniPass key in the system tray. Click **Vault Management**; OmniPass will prompt you to authenticate. Once you gain access to **Vault Management**, click **Manage Identities** under **Vault Settings**. You can only manage the identities of the currently logged in OmniPass user

To add a new identity, click **New Identity** or double-click **Click here to add a new identity**. Name the new identity and click [OK], then click [Apply]. You can now switch to the new identity and start remembering passwords.

To delete an identity, highlight the identity you want to delete and click [Delete Identity], then click [Apply].

When you delete an identity, all of its associated remembered sites and password protected dialogs are lost.

To set the default identity, highlight the identity you want as default and click [Set as Default]; click [Apply] to ensure the settings are saved. If you log in to OmniPass with a fingerprint device, you will automatically be logged in to the default identity for that OmniPass user. You can choose the identity with which you are logging in if you login using "master password".

Choosing User Identity during Login
To choose your identity during login, type your username in the **User Name:** field. Press [Tab] and see that the **Domain:** field self-populates. Click the **Password:** field to bring the cursor to it, and you will see the pull-down menu in the **Identity:** field. Select the identity you wish to login as and then click **OK** to login.

Switch User Identity
To switch identities at any time, right-click the OmniPass system tray icon and click **Switch User Identity** from the submenu. The **Switch Identity** dialog will appear. Select the desired identity and then click **OK**.

Identities and Password Management

On the **Manage Passwords** interface of the **Vault Management** tab of the OmniPass Control Center, there is a pull-down selection box labeled, **Identity**. This field lets you choose which identity you are managing passwords for. When you select an identity here, only those password protected dialogs that are associated with that identity are shown. You can perform all the functions explained in "Password Management" on page 70.

CONFIGURING OMNIPASS

This section gives an overview of both the Export/Import function and the OmniPass Control Center.

Exporting and Importing Users

Using the OmniPass Control Center, you can export and import users in and out of OmniPass. The export process backs up all remembered sites, credentials, and any enrolled fingerprints for an OmniPass user. All OmniPass data for a user is backed up to a single encrypted database file. During the import process, the Windows login of the exported user is required. If the proper credentials cannot be supplied, the user profile will not be imported.

- You should periodically export your user profile and store it in a safe place. If anything happens to your system, you can import your OmniPass profile to a new system and have all your remembered settings and fingerprints instantly.
- When you examine the importation, you are prompted for authentication. The credentials that will allow a user profile to be imported are the Windows login credentials of the exported user. They are the credentials that had to be submitted when the user profile was exported. You will need User Name, Password, and Domain.

Exporting an OmniPass User Profile

To export a user, open the OmniPass Control Center, and click **Import/Export User** under **Manage Users**.

Click **Exports an OmniPass user profile**. OmniPass will prompt you to authenticate. Upon successfully authentication, you must name the OmniPass user profile and decide where to save it. An .opi file is generated, and you should store a copy of it in a safe place.

This .opi file contains all your user specific OmniPass data, and it is both encrypted and password protected. This user profile does NOT contain any of your encrypted data files.

Importing an OmniPass User Profile

You cannot import a user into OmniPass if there already is a user with the same name enrolled in OmniPass.

To import an OmniPass user open the OmniPass Control Center, and click **Import/Export User** under **Manage Users**. Click **Imports a new user into OmniPass** and then select **OmniPass Import/Export File (*.opi)** and click **Next**. OmniPass will then prompt you to browse for the file you had previously exported (.opi file). When you select the .opi file for importation, OmniPass will prompt you for authentication. The credentials that will allow a user profile to be imported are the Windows login credentials of the exported user. They are the credentials that had to be submitted when the user profile was exported. You will need **User Name**, **Password**, and **Domain**. If you don't remember the value for **Domain**, in a PC or SOHO environment **Domain** should be your computer name.

OmniPass will notify you if the user was successfully imported.

Things to Know Regarding Import/Export

- Assume you export a local Windows User profile from OmniPass. You want to import that profile to another machine that has OmniPass. Before you can import the profile, a Windows user with the same login credentials must be created on the machine importing the profile.

  Example: I have a Windows user with the username "Tom" and the password "Sunshine" on my system. I have enrolled Tom into OmniPass and remembered passwords. I want to take all my passwords to new system. I export Tom's OmniPass user profile. I go to my new system and using the Control Panel I create a user with the username "Tom" and the password "Sunshine". I can now successfully import the OmniPass user data to the new system.
- If you export an OmniPass-only user, you can import that user to any computer running OmniPass, provided that a user with that name is not already enrolled in OmniPass.
- If you attempt to import a user profile who has the same name as a user already enrolled in OmniPass, the OmniPass import function will fail.

OMNIPASS CONTROL CENTER

This section will serve to explain functions within the OmniPass Control Center that weren't explained earlier.

You can access the OmniPass Control Center any of three ways:

- Double-click the golden OmniPass key shaped icon in the Windows taskbar (typically in the lower-right corner of the desktop)
- Click the **Start** button; select the **Programs** group; select the **Softex** program group; and click the **OmniPass Control Center** selection.
- Open the Windows **Control Panel** (accessible via **Start** button --> **Settings** --> **Control Panel**) and double-click the **Softex OmniPass** icon.

User Management

The User Management tab has two major interfaces: **Add/Remove User** and **Import/Export User**. Import/Export User functionality is documented in "Exporting and Importing Users" on page 71. Add/Remove User functionality is straightforward.

If you click **Adds a new user to OmniPass** you will start the OmniPass Enrollment Wizard. The Enrollment Wizard is documented in "User Enrollment" on page 68.

If you click **Removes a user from OmniPass**, OmniPass will prompt you to authenticate. Authenticate with the credentials (or enrolled fingerprint) of the user you wish to remove. OmniPass will prompt you to confirm user removal. Click **OK** to complete user removal.

Removing a user will automatically destroy all OmniPass data associated with that user. All identities and credentials associated with the user will be lost. If you are sure about removing the user, we recommend you export the user profile.

User Settings

The User Settings tab has four interfaces: **Audio Settings**, **Taskbar Tips**, and **Enrollment**. User settings allow users to customize OmniPass to suit their individual preferences. Under **User Settings** (**Audio Settings** and **Taskbar Tips**) you can set how OmniPass notifies the user of OmniPass events (e.g., successful login, access denied, etc.). The details of each setting under the **Audio Settings** and **Taskbar Tips** interfaces are self-explanatory.

The **Enrollment** interface allows you to enroll fingerprints. For the procedure to enroll and authentication device refer to *Chapter 2.3*. To enroll additional fingerprints, click **Enroll Authentication Device**, and authenticate with OmniPass. Select the fingerprint recognition device in the **Select Authentication Device** screen (it should already be marked by a green check if you have a finger enrolled) and click **Next**.

System Settings

The OmniPass **Startup Options** interface can be found in the System Settings tab. With these options you can specify how your OmniPass Logon is tied to your Windows Logon.

The first option, **Automatically log on to OmniPass as the current user**, will do just as it says; during Windows login, you will be logged on to OmniPass using your Windows login credentials. If the user logging into Windows was never enrolled into OmniPass, upon login no one will be logged on to OmniPass. This setting is appropriate for an office setting or any setting where users must enter a username and password to log into a computer. This is the default setting.

With the second option, **Manually log on to OmniPass at startup**, OmniPass will prompt you to login once you have logged on to Windows.

With the third option, **Do not log on to OmniPass at startup**, OmniPass will not prompt for a user to be logged on.

You can manually log on to OmniPass by right-clicking the OmniPass taskbar icon and clicking **Log in User** from the right-click menu.

TROUBLESHOOTING

You cannot use OmniPass to create Windows users. You must first create the Windows user, and you will need administrative privileges to do that. Once the Windows user is created, you can add that user to OmniPass using the same username and password

Cannot add Windows users to OmniPass

If you experience difficulties adding a Windows user to OmniPass, you may need to adjust your local security settings. You can do this by going to **Start, Control Panel**, **Administrative Tools,** and **Local Security Settings**. Expand **Local Policies**, expand **Security Options**, and double-click **Network Access: Sharing and Security Model for Local Accounts**. The correct setting should be *Classic - Local Users Authenticate as Themselves*.

Cannot add a User with a Blank Password to OmniPass

If you experience difficulties adding a user with a blank password to OmniPass, you may need to adjust your local security settings. First attempt the procedure explained in the *Cannot add Windows user to OmniPass* section. If the difficulties persist, then try the following procedure.

Click **Start, Control Panel, Administrative Tools,** and **Local Security Settings.** Expand **Local Policies,** expand **Security Options**, and double-click **Accounts: Limit local account use of blank passwords to console login only.** This setting should be set to Disabled.

Dialog appears after OmniPass authentication during Windows Logon

After installing OmniPass on your system, you can choose to logon to Windows using OmniPass. You authenticate with OmniPass (via master password, or an enrolled security device) and OmniPass logs you into Windows. You may, during this OmniPass authentication, see a **Login Error** dialog box.

This dialog box occurs when OmniPass was unable to log you into Windows with the credentials supplied (username and password). This could happen for any of the following reasons:

- Your Windows password has changed
- Your Windows account has been disabled

If you are having difficulties due to the first reason, you will need to update OmniPass with your changed Windows account password. Click **Update Password** and you will be prompted with a dialog to reconfirm your password.

Enter the new password to your Windows user account and click **OK**. If the error persists, then it is unlikely the problem is due to your Windows user account password changing.

Trusted Platform Module Installation

This disc contains several utilities that allow you to enhance the security of your system using the optional Trusted Platform Module (TPM) contained in the system. TPM is a Trusted Computer Group (TCG)-compliant embedded security chip that allows computers to run applications more securely and to make transactions and communications more trustworthy. TPM is an important component of the Fujitsu Security Platform.

- The use of this disc requires that you have a device capable of reading CDs attached to your system. If you do not have a built-in CD or DVD player, you will need to attach an external player.
- The use of this disc **also** requires a device capable of writing to removable media (such as a floppy disk drive, CD-RW drive, or PCMCIA memory card). This drive will be used to store the Emergency Recovery Token file and -- if desired -- the Emergency Recovery Archive file. For more information on available external devices, visit our Web site at: **us.fujitsu.com/computers**.

When installing the software, be sure to create Emergency Recovery Archive and Emergency Recovery Token files when prompted by the Security Platform Initialization Wizard. These files will be necessary in the event of hardware failure. **Failure to create these files could result in a loss of the Security Platform owner key**, which is the physical root for secrets as well as the logical root for all Security Platform user-specific keys. The Initialization Wizard provides step-by-step instructions for creating the files.

Procedure

Be sure you have a built-in or external drive attached to your system that can read CDs. You will also need a means to write to removable media during the installation.

Enabling the Security Chip in BIOS

1. Before installing the TPM software, you will need to enable the security chip in the system BIOS. To do so:
   - If your system is running, click [Start] -> Shut Down, and select Restart. Click [OK].
   - If the system is not running, power it up.
2. When the Fujitsu logo appears, press the [F2] button. The BIOS Setup Utility will appear.
3. Open the Security menu, scroll down to Set Supervisor Password, and enter a password (if not already set).
4. While in the Security menu, scroll down to Security Chip Setting, and click on it. The Security Chip Setting submenu will appear.
5. Click on Security Chip to enable it.
6. Click [F10] to save changes and exit.

Installing the TPM Applications

1. Insert the “Trusted Platform Module Drivers and Applications CD” in the drive.
2. The setup program should start the installation automatically. If the installation does not start automatically, go to the setup.exe file on the disc and double-click on it.
3. Follow the instructions that appear on your screen to load the drivers and applications for TPM.
4. After loading the software, you will be prompted to reboot your system. Remove the CD from the drive, then reboot.
5. After rebooting, the Security Platform Installation Wizard will open and lead you through the setup and customization of the TPM applications.

Getting Help

- For detailed help about installing the TPM applications, go to the readme.txt file on the disc.
- For in-depth help and information about the TPM applications, double-click on the Security Platform icon in the system tray, and click {Getting Started Guide].

Index